

JP09584500

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application: 2002年 8月 7日

出願番号

Application Number: 特願2002-230270

[ ST.10/C ]:

[ JP2002-230270 ]

出願人

Applicant(s): ソニー株式会社

2003年 5月27日

特許長官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3039638

【書類名】 特許願  
【整理番号】 0290478502  
【提出日】 平成14年 8月 7日  
【あて先】 特許庁長官殿  
【国際特許分類】 G09C 1/00  
【発明者】  
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内  
【氏名】 金丸 昌司  
【特許出願人】  
【識別番号】 000002185  
【氏名又は名称】 ソニー株式会社  
【代理人】  
【識別番号】 100093241  
【弁理士】  
【氏名又は名称】 宮田 正昭  
【電話番号】 03-5541-7577  
【選任した代理人】  
【識別番号】 100101801  
【弁理士】  
【氏名又は名称】 山田 英治  
【電話番号】 03-5541-7577  
【選任した代理人】  
【識別番号】 100086531  
【弁理士】  
【氏名又は名称】 澤田 俊夫  
【電話番号】 03-5541-7577  
【手数料の表示】  
【予納台帳番号】 048747

特2002-230270

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号強度指標算出方法、およびコンピュータ・プログラム

【特許請求の範囲】

【請求項1】

暗号処理アルゴリズムの暗号強度指標算出方法であり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値が  $U_i$ , ( $i = 1, 2, \dots$ )、中間値が  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 0, 1, 2, \dots$ )、非線形変換部出力が  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )、前記中間値  $Z_i$ , ( $i = 1, 2, \dots$ )、より生成されるラウンド鍵が  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) と表され、

マスター鍵から初期値  $U_i$ , ( $i = 1, 2, \dots$ ) を生成するステップと、初期値  $U_i$ , ( $i = 1, 2, \dots$ ) から中間値  $Z_i^{(0)}$ , ( $i = 1, 2, \dots$ ) を計算するステップと、中間値  $Z_i^{(r-1)}$ , ( $i = 1, 2, \dots$ ) から中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots$ ) を計算する複数のステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 及び初期値  $U_i$ , ( $i = 1, 2, \dots$ ) から非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を計算するステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) からラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) が前記初期値  $U_i$ , ( $i = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) の線形結合で表記できるように前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 変数を消去するステップと、

前記線形結合式を、右辺が前記初期値  $U_i$ , ( $i = 1, 2, \dots$ ) 及び前記

非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots$ ,  $r = 1, 2, \dots$ ) の項のみを有するように移項した連立線形方程式に変換するステップと、

前記連立線形方程式を行列方程式に変換するステップと、

前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、

前記階段行列の行数から前記階段行列の rank 値を減じた数を N としたとき、変換後の前記行列方程式の左辺の行列の下 N 行からなる新たな行列を生成するステップと、

前記ラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots$ ,  $r = 1, 2, \dots$ ) を要素とする列ベクトルを前記生成された新たな行列に乘すことによって  $N$  個の線形関係式を求めるステップと、

を有することを特徴とする暗号強度指標算出方法。

## 【請求項2】

暗号処理アルゴリズムの暗号強度指標算出処理実行プログラムを記述したコンピュータ・プログラムであり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値が  $U_i$ , ( $i = 1, 2, \dots$ )、中間値が  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 0, 1, 2, \dots$ )、非線形変換部出力が  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )、前記中間値  $Z_i$ , ( $i = 1, 2, \dots$ )、より生成されるラウンド鍵が  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )と表され、

マスター鍵から初期値  $U_i$ , ( $i = 1, 2, \dots$ )、を生成するステップと、初期値  $U_i$ , ( $i = 1, 2, \dots$ )、から中間値  $Z_i^{(0)}$ , ( $i = 1, 2, \dots$ ) を計算するステップと、中間値  $Z_i^{(r-1)}$ , ( $i = 1, 2, \dots$ ) から中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots$ ) を計算する複数のステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )、及び初期値  $U_i$ , ( $i = 1, 2, \dots$ ) から非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を計算するステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )

．．．， $r = 1, 2, \dots$ ）からラウンド鍵 $K_i^{(r)}$ ， $(i = 1, 2, \dots, r = 1, 2, \dots)$ を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵 $K_i^{(r)}$ ， $(i = 1, 2, \dots, r = 1, 2, \dots)$ が前記初期値 $U_i$ ， $(i = 1, 2, \dots)$ 及び前記非線形変換部出力 $V_i^{(r)}$ ， $(i = 1, 2, \dots, r = 1, 2, \dots)$ の線形結合で表記できるように前記中間値 $Z_i^{(r)}$ ， $(i = 1, 2, \dots, r = 1, 2, \dots)$ 変数を消去するステップと、

前記線形結合式を、右辺が前記初期値 $U_i$ ， $(i = 1, 2, \dots)$ 及び前記非線形変換部出力 $V_i^{(r)}$ ， $(i = 1, 2, \dots, r = 1, 2, \dots)$ の項のみを有するように移項した連立線形方程式に変換するステップと、

前記連立線形方程式を行列方程式に変換するステップと、

前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、

前記階段行列の行数から前記階段行列の rank 値を減じた数を N としたとき、変換後の前記行列方程式の左辺の行列の下 N 行からなる新たな行列を生成するステップと、

前記ラウンド鍵 $K_i^{(r)}$ ， $(i = 1, 2, \dots, r = 1, 2, \dots)$ を要素とする列ベクトルを前記生成された新たな行列に乗ずることによって N 個の線形関係式を求めるステップと、

を有することを特徴とするコンピュータ・プログラム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、暗号強度指標算出方法、およびコンピュータ・プログラムに関する。さらに、詳細には、共通鍵ブロック暗号の安全性・強度を評価するための指標を算出する暗号強度指標算出方法、およびコンピュータ・プログラムに関する。

##### 【0002】

**【従来の技術】**

暗号処理アルゴリズムには様々なものがあるが、大きく分類すると、暗号化鍵と復号化鍵を異なる鍵、例えば公開鍵と秘密鍵として設定する公開鍵暗号方式と、暗号化鍵と復号化鍵を共通の鍵として設定する共通鍵暗号方式とに分類される。

**【0003】**

共通鍵暗号方式にも様々なアルゴリズムがあるが、その1つに共通鍵をベースとして複数の鍵を生成して、生成した複数の鍵を用いて暗号処理を実行する方式がある。複数の鍵の生成方式としてラウンド関数を用いる方式がある。これは、共通鍵に対してラウンド関数を作用させ、その出力値をもとに新たな鍵を生成し、さらに出力値にラウンド関数を作用させて得られる次の出力値をもとに次の鍵を生成するといった手順を繰り返して実行することによって複数の鍵を生成する方式である。このような鍵生成方式を適用したアルゴリズムの代表的なものが共通鍵ブロック暗号方式である。

**【0004】**

共通鍵ブロック暗号のアルゴリズムは、主として、ラウンド関数部と鍵スケジュール部とに分けることができる。従来、共通鍵ブロック暗号を設計する際には、鍵関連攻撃等に対する安全性を確保するため、暗号の設計者は、ラウンド鍵間の単純な関係式が成立しないように、注意深く鍵スケジュール部の設計を行うことが要請してきた。

**【0005】**

このような指針に基づいて設計された暗号として、東芝が提案した共通鍵ブロック暗号「Hierocrypt」がある。Hierocryptについては、例えば「"The Block Cipher Hierocrypt ", K.Ohkuma, et al Selected areas in cryptography, LNCS 2012, pp.72-88, 2000.」を参照されたい。Hierocryptの鍵スケジュール部は、Feistel構造と呼ばれる繰り返し構造をもっているが、Feistel構造の右半分の線形変換部に、ラウンド依存定数をXOR加算することによって鍵関連攻撃を回避することを試みている。

**【0006】**

ところが、実際にはHierocryptの作者が予期していなかったラウンド鍵間の線形関係式が成立することが、2001年にFuruya等によって発見された。詳細については、例えば、「S. Furuya and V. Rijmen, Observations on Hierocrypt-3/L1 Key-scheduling Algorithms, Second NESSIE workshop, 2001.」に述べられている。

## 【0007】

## 【発明が解決しようとする課題】

しかし、上述のFuruya等によって行われた手法は、Hierocryptの鍵スケジュール部のアルゴリズムを試行錯誤で組み合わせることによってラウンド鍵間の線形関係式を導出するものであるため、発見された関係式が全てを網羅しているという保証はなかった。更に、試行錯誤的な方法では、鍵スケジュールが一層複雑になった場合、関係式を求めるのは困難を極める。

## 【0008】

本発明は、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することを可能としたものであり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を行なうことを可能とした暗号強度指標算出方法、およびコンピュータ・プログラムを提供することを目的とする。

## 【0009】

## 【課題を解決するための手段】

本発明の第1の側面は、

暗号処理アルゴリズムの暗号強度指標算出方法であり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値が $U_i$ 、( $i = 1, 2, \dots$ )、中間値が $Z_i^{(r)}$ 、( $i = 1, 2, \dots, r = 0, 1, 2, \dots$ )、非線形変換部出力が $V_i^{(r)}$ 、( $i = 1, 2, \dots, r = 1, 2, \dots$ )、前記中間値 $Z_i$ 、( $i = 1, 2, \dots$ )、より生成されるラウンド鍵が $K_i^{(r)}$ 、( $i = 1, 2, \dots, r = 1, 2, \dots$ )と表され、

マスター鍵から初期値 $U_i$ 、( $i = 1, 2, \dots$ )、を生成するステップと

、初期値  $U_i$ , ( $i = 1, 2, \dots$ )、から中間値  $Z_i^{(0)}$ , ( $i = 1, 2, \dots$ ) を計算するステップと、中間値  $Z_i^{(r-1)}$ , ( $i = 1, 2, \dots$ ) から中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots$ ) を計算する複数のステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )、及び初期値  $U_i$ , ( $i = 1, 2, \dots$ ) から非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を計算するステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) からラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) が前記初期値  $U_i$ , ( $i = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) の線形結合で表記できるように前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 変数を消去するステップと、

前記線形結合式を、右辺が前記初期値  $U_i$ , ( $i = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) の項のみを有するように移項した連立線形方程式に変換するステップと、

前記連立線形方程式を行列方程式に変換するステップと、

前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、

前記階段行列の行数から前記階段行列の rank 値を減じた数を N としたとき、変換後の前記行列方程式の左辺の行列の下 N 行からなる新たな行列を生成するステップと、

前記ラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を要素とする列ベクトルを前記生成された新たな行列に乗ずることによって N 個の線形関係式を求めるステップと、

を有することを特徴とする暗号強度指標算出方法にある。

## 【0010】

さらに、本発明の第2の側面は、

暗号処理アルゴリズムの暗号強度指標算出処理実行プログラムを記述したコンピュータ・プログラムであり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値が $U_i$ , ( $i = 1, 2, \dots$ )、中間値が $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 0, 1, 2, \dots$ )、非線形変換部出力が $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )、前記中間値 $Z_i$ , ( $i = 1, 2, \dots$ )、より生成されるラウンド鍵が $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )と表され、

マスター鍵から初期値 $U_i$ , ( $i = 1, 2, \dots$ )、を生成するステップと、初期値 $U_i$ , ( $i = 1, 2, \dots$ )、から中間値 $Z_i^{(0)}$ , ( $i = 1, 2, \dots$ )を計算するステップと、中間値 $Z_i^{(r-1)}$ , ( $i = 1, 2, \dots$ )から中間値 $Z_i^{(r)}$ , ( $i = 1, 2, \dots$ )を計算する複数のステップと、前記中間値 $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )、及び初期値 $U_i$ , ( $i = 1, 2, \dots$ )から非線形変換部出力 $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )を計算するステップと、前記中間値 $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )及び前記非線形変換部出力 $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )からラウンド鍵 $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵 $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )が前記初期値 $U_i$ , ( $i = 1, 2, \dots$ )及び前記非線形変換部出力 $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )の線形結合で表記できるように前記中間値 $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )変数を消去するステップと、

前記線形結合式を、右辺が前記初期値 $U_i$ , ( $i = 1, 2, \dots$ )及び前記非線形変換部出力 $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ )の項の

みを有するように移項した連立線形方程式に変換するステップと、  
 前記連立線形方程式を行列方程式に変換するステップと、  
 前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、  
 前記階段行列の行数から前記階段行列の  $r \ a \ n \ k$  値を減じた数を  $N$  としたとき、変換後の前記行列方程式の左辺の行列の下  $N$  行からなる新たな行列を生成するステップと、  
 前記ラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を要素とする列ベクトルを前記生成された新たな行列に乗ずることによって  $N$  個の線形関係式を求めるステップと、  
 を有することを特徴とするコンピュータ・プログラムにある。

## 【0011】

## 【作用】

本発明の構成によれば、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することが可能となり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を実行することが可能となる。

## 【0012】

本発明の構成によれば、暗号アルゴリズムのうち、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することにより、ラウンド鍵間の全ての線形関係式を求めることが可能となる。

## 【0013】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

## 【0014】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

## 【0015】

## 【発明の実施の形態】

以下、本発明の暗号強度指標算出方法について詳細に説明する。まず、本発明の暗号強度指標算出処理の手順の概略について図1の処理フローを参照して説明する。その後、複数の具体的な共通鍵ブロック暗号アルゴリズムを例として、本発明の暗号強度指標算出処理を実行した例について説明する。

## 【0016】

## 【暗号強度指標算出処理概要】

図1は、本発明の暗号強度指標算出処理の処理手順をフローチャートとして示した図である。各処理ステップの概略について説明する。

## 【0017】

まず、ステップS101では、暗号強度指標算出処理対象となる暗号アルゴリズムを設定する。ここで暗号強度指標算出処理対象となる暗号アルゴリズムは、共通鍵ブロック暗号アルゴリズムである。

## 【0018】

具体的には、線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値が $U_i$ 、( $i = 1, 2, \dots$ )、中間値が $Z_i^{(r)}$ 、( $i = 1, 2, \dots, r = 0, 1, 2, \dots$ )、非線形変換部出力が $V_i^{(r)}$ 、( $i = 1, 2, \dots, r = 1, 2, \dots$ )、前記中間値 $Z_i$ 、( $i = 1, 2, \dots$ )、より生成されるラウンド鍵が $K_i^{(r)}$ 、( $i = 1, 2, \dots, r = 1, 2, \dots$ )と表され、マスター鍵から初期値 $U_i$ 、( $i = 1, 2, \dots$ )、を生成するステップと、初期値 $U_i$ 、( $i = 1, 2, \dots$ )、から中間値 $Z_i^{(0)}$ 、( $i = 1, 2, \dots$ )を計算するステップと、中間値 $Z_i^{(r-1)}$ 、( $i = 1, 2, \dots$ )から中間値 $Z_i^{(r)}$ 、( $i = 1, 2, \dots$ )を計算する

複数のステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 及び初期値  $U_i$ , ( $i = 1, 2, \dots$ ) から非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を計算するステップと、前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) からラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定する。

## 【0019】

次に、ステップ S102において、ステップ S101において設定した共通鍵ブロック暗号処理アルゴリズムの中間変数を消去する。すなわち、ラウンド鍵  $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) が前記初期値  $U_i$ , ( $i = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) の線形結合で表記できるように前記中間値  $Z_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) 変数を消去する処理を実行する。具体的な処理例については後述する。

## 【0020】

次にステップ S103において、変数移項処理を実行する。すなわち、前記線形結合式を、右辺が前記初期値  $U_i$ , ( $i = 1, 2, \dots$ ) 及び前記非線形変換部出力  $V_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) の項のみを有するように移項した連立線形方程式に変換する処理を実行する。具体的な処理例については後述する。

## 【0021】

次に、ステップ S104において、行列方程式変換処理を実行する。すなわち、前記連立線形方程式を行列方程式に変換する処理を実行する。具体的な処理例については後述する。

## 【0022】

次に、ステップ S105において、ユニタリ変換処理を実行する。すなわち、前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列

を左から乗じる処理を実行する。具体的な処理例については後述する。

#### 【0023】

次にステップS106において、小行列選択処理を実行する。すなわち、前記階段行列の行数から前記階段行列のrank値を減じた数をNとしたとき、変換後の前記行列方程式の左辺の行列の下N行からなる新たな行列を生成する。具体的な処理例については後述する。

#### 【0024】

次にステップS107において、線形関係式生成処理を実行する。すなわち、前記ラウンド鍵 $K_i^{(r)}$ , ( $i = 1, 2, \dots, r = 1, 2, \dots$ ) を要素とする列ベクトルを前記生成された新たな行列に乗することによってN個の線形関係式を求める。具体的な処理例については後述する。

#### 【0025】

上述した処理によって求められた線形関係式の数：NをステップS101において設定した共通鍵ブロック暗号アルゴリズムの暗号強度指標とするものである。上述した処理フローは、ステップS101において設定した共通鍵ブロック暗号アルゴリズムのラウンド鍵間の線形関係式を網羅する線形関係式の数：Nを求める処理として実行され、線形関係式の数：Nが大であるほど暗号強度が弱く、小であるほど暗号強度が強いとの判定が可能である。従って、図1に示すフローに従って求められる線形関係式数：Nを共通鍵ブロック暗号アルゴリズムの暗号強度指標として適用することが可能となる。

#### 【0026】

図1に示す処理手順に従った処理によれば、暗号アルゴリズムのうち、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することでラウンド鍵間の全ての線形関係式を求めることが可能となる。

#### 【0027】

##### [暗号強度指標算出処理具体例1]

次に、本発明に係る暗号強度指標算出処理具体例として、東芝から提案されたブロック暗号「Hierocrypt-L1」に対して本発明に係る暗号強度評価方法を適用

した処理例の詳細について説明する。Hierocrypt-L1は、ブロック長さ64bit、鍵長128bitの共通鍵ブロック暗号である。

## 【0028】

まず、図1に示すステップS101の暗号処理アルゴリズムの設定ステップについて説明する。ここでは、東芝から提案されたブロック暗号「Hierocrypt-L1」の設定処理として実行する。

## 【0029】

$O_n$ ,  $I_n$ を各々n行n列の零行列、単位行列とする。これを用いて、行列P<sub>16</sub>は以下のように定義される。

## 【0030】

## 【数1】

$$P_{16} = \begin{pmatrix} I_2 & O_2 & I_2 & O_2 \\ O_2 & I_2 & O_2 & I_2 \\ O_2 & I_2 & I_2 & I_2 \\ I_2 & O_2 & I_2 & I_2 \end{pmatrix}$$

## 【0031】

また、行列P<sub>16</sub><sup>-1</sup>を、行列P<sub>16</sub>の逆行列とする。次に、行列M<sub>5</sub>、MBを以下のように定義する。

## 【0032】

## 【数2】

$$M_5 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$MB = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

## 【0033】

さらに、行列M<sub>5</sub>、MBを用いて、以下のように行列M<sub>5B</sub>、MB<sub>5</sub>を定義する。

## 【0034】

## 【数3】

$$\begin{aligned} M5B &= \begin{pmatrix} M5 & O4 \\ O4 & MB \end{pmatrix} \\ MB5 &= \begin{pmatrix} MB & O4 \\ O4 & M5 \end{pmatrix} \end{aligned}$$

## 【0035】

次に、ラウンド依存定数ベクトルG i ((i = 0 . . . 7) を以下のように定義する。

## 【0036】

## 【数4】

G 0 = (h01, h02, h03, h04, 0, 0, 0, 0)  
 G 1 = (h11, h12, h13, h14, 0, 0, 0, 0)  
 G 2 = (h21, h22, h23, h24, 0, 0, 0, 0)  
 G 3 = (h31, h32, h33, h34, 0, 0, 0, 0)  
 G 4 = (h41, h42, h43, h44, 0, 0, 0, 0)  
 G 5 = (h41, h42, h43, h44, 0, 0, 0, 0)  
 G 6 = (h31, h32, h33, h34, 0, 0, 0, 0)  
 G 7 = (h21, h22, h23, h24, 0, 0, 0, 0)

## 【0037】

なお、上式で用いられている定数を要素とするベクトルHHを、以下のように定義しておく。

## 【0038】

## 【数5】

HH=(h01, h02, h03, h04, h11, h12, h13, h14, h21, h22, h23, h24, h31, h32, h33, h34, h41, h42, h43, h44)

## 【0039】

具体的な、h01, h02, . . . , h44の値は、以下のように定義される。

## 【0040】

## 【数6】

(h01,h01,h02,h03)=(0x5a, 0x82, 0x79, 0x99 )  
 (h11,h11,h12,h13)=(0x6e, 0xd9, 0xeb, 0xa1 )  
 (h21,h21,h22,h23)=(0x8f, 0x1b, 0xbc, 0xdc )  
 (h31,h31,h32,h33)=(0xca, 0x62, 0xc1, 0xd6 )  
 (h41,h41,h42,h43)=( 0xf7, 0xde, 0xf5, 0x8a )

## 【0041】

次に、鍵スケジュール部の初期値の右半分から成るベクトルZZを、以下のように定義する。

## 【0042】

## 【数7】

ZZ=(z31,z32,z33,z34,z41,z42,z43,z44)

## 【0043】

これらを用いて、共通鍵暗号アルゴリズムHierocrypt-L1の鍵スケジュール部の右半分は、以下のように表せる。なお、演算子+は、ガロア体GF(2)上の加法演算子である。

## 【0044】

## 【数8】

Z0=M5B\*ZZ+G0

W0=P16\*Z0

Z1=M5B\*W0+G1

W1=P16\*Z1

Z2=M5B\*W1+G2

W2=P16\*Z2

Z3=M5B\*W2+G3

W3=P16\*Z3

Z4=M5B\*W3+G4

W5=MB5\*(Z4+G5)

Z5=P16I\*W5

W6=MB5\*(Z5+G6)

$Z_6 = P16I * W6$

$W7 = MB5 * (Z6 + G7)$

$Z7 = P16I * W7$

【0045】

ここで、 $Z0, Z1, Z2, Z3, Z4, Z5, Z6, Z7, W0, W1, W2, W3, W5, W6, W7$ は、鍵スケジュール部の中間値の右半分を表す。

【0046】

次に、これらの中間値を、下式、

【0047】

【数9】

$Zn = Zn_3 || Zn_4$

$Wn = Wn_1 || WN_2$

【0048】

のように分割して表現する。但し記号 “||” は、ベクトルの連結を表す。

【0049】

次に、各ラウンドの非線形変換部出力を、 $V0, V1, V2, V3, V4, V5, V6, V7$ とする。

但し、各々は、下記に示す4つの要素から成るベクトルである。

【0050】

【数10】

$V0 = (v01, v02, v03, v04)$

$V1 = (v11, v12, v13, v14)$

$V2 = (v21, v22, v23, v24)$

$V3 = (v31, v32, v33, v34)$

$V4 = (v41, v42, v43, v44)$

$V5 = (v51, v52, v53, v54)$

$V6 = (v61, v62, v63, v64)$

$V7 = (v71, v72, v73, v74)$

【0051】

ここで、ベクトル  $Z_1, Z_2$  を下記のように設定する。

【0052】

【数11】

$$Z_1 = (z_{11}, z_{12}, z_{13}, z_{14})$$

$$Z_2 = (z_{21}, z_{22}, z_{23}, z_{24})$$

【0053】

上記のように、ベクトル  $Z_1$ 、 $Z_2$  を設定すると、Hierocrypt-L1 の鍵スケジュール部の左半分は、以下のように表せる。

【0054】

【数12】

$$Z_{01} = Z_2$$

$$Z_{02} = Z_1 + V_0$$

$$Z_{11} = Z_{02}$$

$$Z_{12} = Z_{01} + V_1$$

$$Z_{21} = Z_{12}$$

$$Z_{22} = Z_{11} + V_2$$

$$Z_{31} = Z_{22}$$

$$Z_{32} = Z_{21} + V_3$$

$$Z_{41} = Z_{32}$$

$$Z_{42} = Z_{31} + V_4$$

$$Z_{51} = Z_{42} + V_5$$

$$Z_{52} = Z_{41}$$

$$Z_{61} = Z_{52} + V_6$$

$$Z_{62} = Z_{51}$$

$$Z_{71} = Z_{62} + V_7$$

$$Z_{72} = Z_{61}$$

【0055】

ここで、 $Z_{01}$ 、 $Z_{02}$ 、 $Z_{11}$ 、 $Z_{12}$ 、 $Z_{21}$ 、 $Z_{22}$ 、 $Z_{31}$ 、 $Z_{32}$ 、 $Z_{41}$ 、 $Z_{42}$ 、 $Z_{51}$ 、 $Z_{52}$ 、 $Z_{61}$ 、 $Z_{62}$ 、 $Z_{71}$ 、 $Z_{72}$  は、鍵スケジュール部の中間値の左半分を表す。

## 【0056】

こうして得られた中間値を用いて、ラウンド鍵： $K1_1, K1_2, K1_3, K1_4$   
 $, K2_1, \dots, K7_1, K7_2$ は、以下のように表せる。

## 【0057】

## 【数13】

$$K1_1 = Z0_1 + V1$$

$$K1_2 = Z1_3 + V1$$

$$K1_3 = Z1_4 + V1$$

$$K1_4 = Z0_2 + Z1_4$$

$$K2_1 = Z1_1 + V2$$

$$K2_2 = Z2_3 + V2$$

$$K2_3 = Z2_4 + V2$$

$$K2_4 = Z1_2 + Z2_4$$

$$K3_1 = Z2_1 + V3$$

$$K3_2 = Z3_3 + V3$$

$$K3_3 = Z3_4 + V3$$

$$K3_4 = Z2_2 + Z3_4$$

$$K4_1 = Z3_1 + V4$$

$$K4_2 = Z4_3 + V4$$

$$K4_3 = Z4_4 + V4$$

$$K4_4 = Z3_2 + Z4_4$$

$$K5_1 = Z5_1 + Z4_3$$

$$K5_2 = W5_1 + V5$$

$$K5_3 = W5_2 + V5$$

$$K5_4 = Z4_1 + W5_2$$

$$K6_1 = Z6_1 + Z5_3$$

$$K6_2 = W6_1 + V6$$

$$K6_3 = W6_2 + V6$$

$$K6_4 = Z5_1 + W6_2$$

$$K7_1 = Z7_1 + Z6_3$$

$$K7_2 = W7_1 + V7$$

$$K7_3 = W7_2 + V7$$

$$K7_4 = Z6_1 + W7_2$$

【0058】

なお、 $K1_1, K1_2, K1_3, K1_4, K2_1, \dots, K7_1, K7_2$ は、4つの要素から成るベクトルである。

【0059】

次に、図1に示すステップS102の中間変数消去処理ステップについて説明する。上述の4つの要素から成るベクトル $K1_1, K1_2, K1_3, K1_4, K2_1, \dots, K7_1, K7_2$ について、実際に各値を代入して計算すると、以下のような式が得られる。

【0060】

【数 1 4】

$$\begin{aligned}
 K_{11} &= \begin{pmatrix} v_{11} + z_{21} \\ v_{12} + z_{22} \\ v_{13} + z_{23} \\ v_{14} + z_{24} \end{pmatrix} \\
 K_{12} &= \begin{pmatrix} h_{01} + h_{11} + h_{03} + v_{11} + z_{32} + z_{41} \\ h_{01} + h_{02} + h_{12} + h_{04} + v_{12} + z_{33} + z_{42} \\ h_{01} + h_{02} + h_{03} + h_{13} + v_{13} + z_{31} + z_{34} + z_{43} \\ h_{02} + h_{04} + h_{14} + v_{14} + z_{31} + z_{44} \end{pmatrix} \\
 K_{13} &= \begin{pmatrix} h_{02} + h_{04} + v_{11} + z_{31} \\ h_{01} + h_{03} + v_{12} + z_{32} \\ h_{02} + h_{03} + h_{04} + v_{13} + z_{32} + z_{41} + z_{33} \\ h_{01} + h_{02} + h_{03} + v_{14} + z_{31} + z_{34} + z_{44} \end{pmatrix} \\
 K_{14} &= \begin{pmatrix} h_{02} + h_{04} + v_{01} + z_{11} + z_{31} \\ h_{01} + h_{03} + v_{02} + z_{12} + z_{32} \\ h_{02} + h_{03} + h_{04} + v_{03} + z_{13} + z_{32} + z_{41} + z_{33} \\ h_{01} + h_{02} + h_{03} + v_{04} + z_{31} + z_{14} + z_{34} + z_{44} \end{pmatrix} \\
 K_{21} &= \begin{pmatrix} v_{01} + v_{21} + z_{11} \\ v_{02} + v_{22} + z_{12} \\ v_{03} + v_{23} + z_{13} \\ v_{04} + v_{24} + z_{14} \end{pmatrix} \\
 K_{22} &= \begin{pmatrix} h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + v_{21} + z_{33} + z_{34} + z_{43} \\ h_{11} + h_{03} + h_{12} + h_{04} + h_{22} + h_{14} + v_{22} + z_{31} + z_{41} + z_{33} + z_{42} + z_{34} \\ h_{11} + h_{12} + h_{04} + h_{13} + h_{23} + v_{23} + z_{32} + z_{42} + z_{34} + z_{43} \\ h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + v_{24} + z_{32} + z_{33} + z_{42} + z_{34} \end{pmatrix} \\
 K_{23} &= \begin{pmatrix} h_{01} + h_{12} + h_{14} + v_{21} + z_{31} + z_{33} + z_{42} + z_{44} \\ h_{02} + h_{11} + h_{13} + v_{22} + z_{31} + z_{32} + z_{41} + z_{34} + z_{43} \\ h_{02} + h_{12} + h_{13} + h_{14} + v_{23} + z_{31} + z_{32} + z_{41} + z_{42} + z_{34} + z_{43} + z_{44} \\ h_{01} + h_{02} + h_{11} + h_{12} + h_{04} + h_{13} + v_{24} + z_{41} + z_{33} + z_{42} + z_{43} + z_{44} \end{pmatrix} \\
 K_{24} &= \begin{pmatrix} h_{01} + h_{12} + h_{14} + v_{11} + z_{21} + z_{31} + z_{33} + z_{42} + z_{44} \\ h_{02} + h_{11} + h_{13} + v_{12} + z_{22} + z_{31} + z_{32} + z_{41} + z_{34} + z_{43} \\ h_{02} + h_{12} + h_{13} + h_{14} + v_{13} + z_{31} + z_{23} + z_{32} + z_{41} + z_{42} + z_{34} + z_{43} + z_{44} \\ h_{01} + h_{02} + h_{11} + h_{12} + h_{04} + h_{13} + v_{14} + z_{41} + z_{24} + z_{33} + z_{42} + z_{43} + z_{44} \end{pmatrix}
 \end{aligned}$$

$$\begin{aligned}
K3_1 &= \begin{pmatrix} v11 + v31 + z21 \\ v12 + v32 + z22 \\ v13 + v33 + z23 \\ v14 + v34 + z24 \end{pmatrix} \\
K3_2 &= \begin{pmatrix} h01 + h03 + h12 + h21 + h04 + h13 + h31 + h23 + v31 + z41 + z42 + z34 + z43 \\ h01 + h21 + h13 + h22 + h14 + h32 + h24 + v32 + z31 + z41 + z33 + z43 \\ h01 + h02 + h21 + h22 + h14 + h23 + h33 + v33 + z32 + z41 + z33 + z34 \\ h02 + h11 + h03 + h12 + h22 + h24 + h34 + v34 + z41 + z33 + z42 + z34 + z44 \end{pmatrix} \\
K3_3 &= \begin{pmatrix} h01 + h02 + h11 + h03 + h04 + h22 + h24 + v31 + z31 + z32 + z41 \\ h02 + h03 + h12 + h21 + h04 + h23 + v32 + z32 + z33 + z42 \\ h03 + h12 + h22 + h23 + h24 + v33 + z31 + z32 + z33 + z42 \\ h01 + h02 + h11 + h12 + h21 + h04 + h22 + h14 + h23 + v34 + z41 + z33 + z42 + z44 \end{pmatrix} \\
K3_4 &= \begin{pmatrix} h01 + h02 + h11 + h03 + h04 + h22 + h24 + v01 + v21 + z11 + z31 + z32 + z41 \\ h02 + h03 + h12 + h21 + h04 + h23 + v02 + v22 + z12 + z32 + z33 + z42 \\ h03 + h12 + h22 + h23 + h24 + v03 + v23 + z13 + z31 + z32 + z33 + z42 \\ h01 + h02 + h11 + h12 + h21 + h04 + h22 + h14 + h23 + v04 + v24 + z14 + z41 + z33 \\ +z42 + z44 \end{pmatrix} \\
k4_1 &= \begin{pmatrix} v01 + v21 + v41 + z11 \\ v02 + v22 + v42 + z12 \\ v03 + v23 + v43 + z13 \\ v04 + v24 + v44 + z14 \end{pmatrix} \\
k4_2 &= \begin{pmatrix} h01 + h11 + h03 + h13 + h22 + h31 + h14 + h23 + h41 + h33 + v41 + z32 + z41 + z43 \\ h11 + h31 + h23 + h32 + h24 + h42 + h34 + v42 + z41 \\ h02 + h11 + h12 + h04 + h31 + h32 + h24 + h33 + h43 + v43 + z31 + z42 \\ h02 + h12 + h21 + h13 + h22 + h32 + h34 + h44 + v44 + z31 + z32 + z41 + z42 + z34 \\ +z43 \end{pmatrix} \\
k4_3 &= \begin{pmatrix} h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + h32 + h34 + v41 + z31 + z42 + z34 \\ +z43 + z44 \\ h02 + h03 + h12 + h04 + h13 + h22 + h31 + h14 + h33 + v42 + z32 + z33 + z42 + z43 \\ h01 + h02 + h03 + h04 + h13 + h22 + h32 + h34 + v43 + z31 + z32 + z43 + z44 \\ h02 + h11 + h12 + h21 + h04 + h22 + h31 + h14 + h32 + h24 + h33 + v44 + z31 + z42 \\ +z44 \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
k_{4_4} &= \left( \begin{array}{l} h_{01} + h_{02} + h_{11} + h_{03} + h_{12} + h_{21} + h_{13} + h_{14} + h_{32} + h_{34} + v_{11} + v_{31} + z_{21} + z_{31} \\ + z_{42} + z_{34} + z_{43} + z_{44} \\ h_{02} + h_{03} + h_{12} + h_{04} + h_{13} + h_{22} + h_{31} + h_{14} + h_{33} + v_{12} + v_{32} + z_{22} + z_{32} + z_{33} \\ + z_{42} + z_{43} \\ h_{01} + h_{02} + h_{03} + h_{04} + h_{13} + h_{22} + h_{32} + h_{33} + h_{34} + v_{13} + v_{33} + z_{31} + z_{23} + z_{32} \\ + z_{43} + z_{44} \\ h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{31} + h_{14} + h_{32} + h_{24} + h_{33} + v_{14} + v_{34} + z_{31} \\ + z_{24} + z_{42} + z_{44} \\ h_{01} + h_{11} + h_{03} + h_{13} + h_{22} + h_{31} + h_{14} + h_{23} + h_{41} + h_{33} + v_{01} + v_{21} + v_{41} + v_{51} \\ + z_{11} + z_{32} + z_{41} + z_{43} \\ h_{11} + h_{31} + h_{23} + h_{32} + h_{24} + h_{42} + h_{34} + v_{02} + v_{22} + v_{42} + v_{52} + z_{12} + z_{41} \\ h_{02} + h_{11} + h_{12} + h_{04} + h_{31} + h_{32} + h_{24} + h_{33} + h_{43} + v_{03} + v_{23} + v_{43} + v_{53} + z_{13} \\ + z_{31} + z_{42} \\ h_{02} + h_{12} + h_{21} + h_{13} + h_{22} + h_{32} + h_{34} + h_{44} + v_{04} + v_{24} + v_{44} + z_{31} + v_{54} + z_{14} \\ + z_{32} + z_{41} + z_{42} + z_{34} + z_{43} \\ h_{02} + h_{11} + h_{12} + h_{21} + h_{13} + h_{22} + h_{31} + h_{23} + h_{24} + v_{51} + z_{31} + z_{32} + z_{42} + z_{34} \\ + z_{43} \\ h_{01} + h_{02} + h_{03} + h_{12} + h_{04} + h_{13} + h_{22} + h_{14} + h_{23} + h_{32} + h_{24} + v_{52} + z_{31} + z_{32} \\ + z_{41} + z_{42} + z_{43} \\ h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{14} + h_{24} + h_{33} + v_{53} + z_{31} + z_{41} + z_{42} + z_{34} \\ h_{01} + h_{03} + h_{21} + h_{04} + h_{14} + h_{23} + h_{24} + h_{34} + v_{54} + z_{34} \\ h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{33} + v_{51} + z_{32} + z_{42} + z_{34} \\ h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + h_{34} + v_{52} + z_{32} + z_{33} + z_{42} + z_{34} \\ h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + h_{31} + v_{53} + z_{33} + z_{34} + z_{43} \\ h_{11} + h_{03} + h_{21} + h_{13} + h_{32} + h_{24} + z_{31} + v_{54} + z_{32} + z_{33} + z_{43} + z_{44} \\ h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{33} + v_{11} + v_{31} + z_{21} + z_{32} + z_{42} + z_{34} \\ h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + h_{34} + v_{12} + v_{32} + z_{22} + z_{32} + z_{33} + z_{42} + z_{34} \\ h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + h_{31} + v_{13} + v_{33} + z_{23} + z_{33} + z_{34} + z_{43} \\ h_{11} + h_{03} + h_{21} + h_{13} + h_{32} + h_{24} + v_{14} + v_{34} + z_{31} + z_{32} + z_{24} + z_{33} + z_{43} + z_{44} \\ h_{01} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{31} + h_{23} + v_{11} + v_{31} + v_{61} + z_{21} + z_{41} + z_{42} \\ + z_{34} + z_{43} \\ h_{01} + h_{21} + h_{13} + h_{22} + h_{14} + h_{32} + h_{24} + v_{12} + v_{32} + v_{62} + z_{22} + z_{31} + z_{41} + z_{33} \\ + z_{43} \\ h_{01} + h_{02} + h_{21} + h_{22} + h_{14} + h_{23} + h_{33} + v_{13} + v_{33} + v_{63} + z_{23} + z_{32} + z_{41} + z_{33} \\ + z_{34} \\ h_{02} + h_{11} + h_{03} + h_{12} + h_{22} + h_{24} + h_{34} + v_{14} + v_{34} + z_{41} + v_{64} + z_{24} + z_{33} + z_{42} \\ + z_{34} + z_{44} \end{array} \right) \\
K_{5_1} &= \left( \begin{array}{l} h_{11} + h_{31} + h_{23} + h_{32} + h_{24} + h_{42} + h_{34} + v_{02} + v_{22} + v_{42} + v_{52} + z_{12} + z_{41} \\ h_{02} + h_{11} + h_{12} + h_{04} + h_{31} + h_{32} + h_{24} + h_{33} + h_{43} + v_{03} + v_{23} + v_{43} + v_{53} + z_{13} \\ + z_{31} + z_{42} \\ h_{02} + h_{12} + h_{21} + h_{13} + h_{22} + h_{32} + h_{34} + h_{44} + v_{04} + v_{24} + v_{44} + z_{31} + v_{54} + z_{14} \\ + z_{32} + z_{41} + z_{42} + z_{34} + z_{43} \end{array} \right) \\
K_{5_2} &= \left( \begin{array}{l} h_{02} + h_{11} + h_{12} + h_{21} + h_{13} + h_{22} + h_{31} + h_{23} + h_{24} + v_{51} + z_{31} + z_{32} + z_{42} + z_{34} \\ + z_{43} \\ h_{01} + h_{02} + h_{03} + h_{12} + h_{04} + h_{13} + h_{22} + h_{14} + h_{23} + h_{32} + h_{24} + v_{52} + z_{31} + z_{32} \\ + z_{41} + z_{42} + z_{43} \\ h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{14} + h_{24} + h_{33} + v_{53} + z_{31} + z_{41} + z_{42} + z_{34} \\ h_{01} + h_{03} + h_{21} + h_{04} + h_{14} + h_{23} + h_{24} + h_{34} + v_{54} + z_{34} \end{array} \right) \\
K_{5_3} &= \left( \begin{array}{l} h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{33} + v_{51} + z_{32} + z_{42} + z_{34} \\ h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + h_{34} + v_{52} + z_{32} + z_{33} + z_{42} + z_{34} \\ h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + h_{31} + v_{53} + z_{33} + z_{34} + z_{43} \\ h_{11} + h_{03} + h_{21} + h_{13} + h_{32} + h_{24} + z_{31} + v_{54} + z_{32} + z_{33} + z_{43} + z_{44} \end{array} \right) \\
K_{5_4} &= \left( \begin{array}{l} h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{33} + v_{11} + v_{31} + z_{21} + z_{32} + z_{42} + z_{34} \\ h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + h_{34} + v_{12} + v_{32} + z_{22} + z_{32} + z_{33} + z_{42} + z_{34} \\ h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + h_{31} + v_{13} + v_{33} + z_{23} + z_{33} + z_{34} + z_{43} \\ h_{11} + h_{03} + h_{21} + h_{13} + h_{32} + h_{24} + v_{14} + v_{34} + z_{31} + z_{32} + z_{24} + z_{33} + z_{43} + z_{44} \end{array} \right) \\
K_{6_1} &= \left( \begin{array}{l} h_{01} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{31} + h_{23} + v_{11} + v_{31} + v_{61} + z_{21} + z_{41} + z_{42} \\ + z_{34} + z_{43} \\ h_{01} + h_{21} + h_{13} + h_{22} + h_{14} + h_{23} + h_{33} + v_{13} + v_{33} + v_{63} + z_{23} + z_{32} + z_{41} + z_{33} \\ + z_{34} \\ h_{02} + h_{11} + h_{03} + h_{12} + h_{22} + h_{24} + h_{34} + v_{14} + v_{34} + z_{41} + v_{64} + z_{24} + z_{33} + z_{42} \\ + z_{34} + z_{44} \end{array} \right)
\end{aligned}$$

$$\begin{aligned}
K_{6_2} &= \left( \begin{array}{l} h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + v61 + z31 + z42 + z34 + z43 + z44 \\ h02 + h03 + h12 + h04 + h13 + h22 + h14 + v62 + z32 + z33 + z42 + z43 \\ h02 + h11 + h04 + h14 + h23 + z31 + v63 + z41 + z44 \\ h11 + h04 + h13 + h14 + h24 + z32 + z41 + v64 + z34 + z43 + z44 \end{array} \right) \\
K_{6_3} &= \left( \begin{array}{l} h01 + h02 + h11 + h12 + h04 + h23 + v61 + z41 + z33 + z42 \\ h02 + h04 + h14 + h24 + v62 + z31 + z44 \\ h01 + h11 + h03 + h21 + v63 + z32 + z41 \\ h01 + h11 + h03 + h22 + h14 + z32 + z41 + v64 + z44 \end{array} \right) \\
K_{6_4} &= \left( \begin{array}{l} h01 + h02 + h11 + h12 + h04 + h23 + v01 + v21 + v41 + v51 + z11 + z41 + z33 + z42 \\ h02 + h04 + h14 + h24 + v02 + v22 + v42 + v52 + z12 + z31 + z44 \\ h01 + h11 + h03 + h21 + v03 + v23 + v43 + v53 + z13 + z32 + z41 \\ h01 + h11 + h03 + h22 + h14 + v04 + v24 + v44 + v54 + z14 + z32 + z41 + z44 \end{array} \right) \\
K_{7_1} &= \left( \begin{array}{l} h02 + h11 + h03 + h21 + h13 + v01 + v21 + v41 + v51 + z11 + v71 + z33 + z34 + z43 \\ h11 + h03 + h12 + h04 + h22 + h14 + v02 + v22 + v42 + v52 + z12 + z31 + v72 + z41 \\ +z33 + z42 + z34 \\ h11 + h12 + h04 + h13 + h23 + v03 + v23 + v43 + v53 + z13 + z32 + v73 + z42 + z34 \\ +z43 \\ h01 + h02 + h12 + h14 + h24 + v04 + v24 + v44 + v54 + z14 + z32 + z33 + z42 + v74 \\ +z34 \end{array} \right) \\
K_{7_2} &= \left( \begin{array}{l} h01 + h02 + h11 + h03 + h04 + v71 + z31 + z32 + z41 \\ h02 + h03 + h12 + h04 + v72 + z32 + z33 + z42 \\ h01 + h04 + h13 + z31 + z32 + z41 + v73 + z33 + z34 + z43 \\ h01 + h03 + h04 + h14 + v74 + z34 \end{array} \right)
\end{aligned}$$

## 【0061】

次に、ステップS103の変数移項処理を実行する。上記K<sub>1,1</sub>, K<sub>1,2</sub>, K<sub>1,3</sub>, K<sub>1,4</sub>, K<sub>2,1</sub>, ..., K<sub>7,1</sub>, K<sub>7,2</sub>の結果に基づいて、上記の連立線形方程式を変形し、右辺がz×x, v×xの項のみを含むように変形すると、以下のように表すことができる。

## 【0062】

【数 1 5】

$$\begin{aligned}
 k_{111} &= v_{11} + z_{21} \\
 k_{112} &= v_{12} + z_{22} \\
 k_{113} &= v_{13} + z_{23} \\
 k_{114} &= v_{14} + z_{24} \\
 h_{01} + h_{11} + h_{03} + k_{121} &= v_{11} + z_{32} + z_{41} \\
 h_{01} + h_{02} + h_{12} + h_{04} + k_{122} &= v_{12} + z_{33} + z_{42} \\
 h_{01} + h_{02} + h_{03} + h_{13} + k_{123} &= v_{13} + z_{31} + z_{34} + z_{43} \\
 h_{02} + h_{04} + h_{14} + k_{124} &= v_{14} + z_{31} + z_{44} \\
 h_{02} + h_{04} + k_{131} &= v_{11} + z_{31} \\
 h_{01} + h_{03} + k_{132} &= v_{12} + z_{32} \\
 h_{02} + h_{03} + h_{04} + k_{133} &= v_{13} + z_{32} + z_{41} + z_{33} \\
 h_{01} + h_{02} + h_{03} + k_{134} &= v_{14} + z_{31} + z_{34} + z_{44} \\
 h_{02} + h_{04} + k_{141} &= v_{01} + z_{11} + z_{31}
 \end{aligned}$$

$$\begin{aligned}
& h_{01} + h_{03} + k_{142} = v_{02} + z_{12} + z_{32} \\
& h_{02} + h_{03} + h_{04} + k_{143} = v_{03} + z_{13} + z_{32} + z_{41} + z_{33} \\
& h_{01} + h_{02} + h_{03} + k_{144} = v_{04} + z_{31} + z_{14} + z_{34} + z_{44} \\
& k_{211} = v_{01} + v_{21} + z_{11} \\
& k_{212} = v_{02} + v_{22} + z_{12} \\
& k_{213} = v_{03} + v_{23} + z_{13} \\
& k_{214} = v_{04} + v_{24} + z_{14} \\
& h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + k_{221} = v_{21} + z_{33} + z_{34} + z_{43} \\
& h_{11} + h_{03} + h_{12} + h_{04} + h_{22} + h_{14} + k_{222} = v_{22} + z_{31} + z_{41} + z_{33} + z_{42} + z_{34} \\
& h_{11} + h_{12} + h_{04} + h_{13} + h_{23} + k_{223} = v_{23} + z_{32} + z_{42} + z_{34} + z_{43} \\
& h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + k_{224} = v_{24} + z_{32} + z_{33} + z_{42} + z_{34} \\
& h_{01} + h_{12} + h_{14} + k_{231} = v_{21} + z_{31} + z_{33} + z_{42} + z_{44} \\
& h_{02} + h_{11} + h_{13} + k_{232} = v_{22} + z_{31} + z_{32} + z_{41} + z_{34} + z_{43} \\
& h_{02} + h_{12} + h_{13} + h_{14} + k_{233} = v_{23} + z_{31} + z_{32} + z_{41} + z_{42} + z_{43} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{04} + h_{13} + k_{234} = v_{24} + z_{41} + z_{33} + z_{42} + z_{43} + z_{44} \\
& h_{01} + h_{12} + h_{14} + k_{241} = v_{11} + z_{21} + z_{31} + z_{33} + z_{42} + z_{44} \\
& h_{02} + h_{11} + h_{13} + k_{242} = v_{12} + z_{22} + z_{31} + z_{32} + z_{41} + z_{34} + z_{43} \\
& h_{02} + h_{12} + h_{13} + h_{14} + k_{243} = v_{13} + z_{31} + z_{23} + z_{32} + z_{41} + z_{42} + z_{34} + \\
& z_{43} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{04} + h_{13} + k_{244} = v_{14} + z_{41} + z_{24} + z_{33} + z_{42} + \\
& z_{43} + z_{44} \\
& k_{311} = v_{11} + v_{31} + z_{21} \\
& k_{312} = v_{12} + v_{32} + z_{22} \\
& k_{313} = v_{13} + v_{33} + z_{23} \\
& k_{314} = v_{14} + v_{34} + z_{24} \\
& h_{01} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{31} + h_{23} + k_{321} = v_{31} + z_{41} + \\
& z_{42} + z_{34} + z_{43} \\
& h_{01} + h_{21} + h_{13} + h_{22} + h_{14} + h_{32} + h_{24} + k_{322} = v_{32} + z_{31} + z_{41} + z_{33} + z_{43} \\
& h_{01} + h_{02} + h_{21} + h_{22} + h_{14} + h_{23} + h_{33} + k_{323} = v_{33} + z_{32} + z_{41} + z_{33} + z_{34} \\
& h_{02} + h_{11} + h_{03} + h_{12} + h_{22} + h_{24} + h_{34} + k_{324} = v_{34} + z_{41} + z_{33} + \\
& z_{42} + z_{34} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{04} + h_{22} + h_{24} + k_{331} = v_{31} + z_{31} + z_{32} + z_{41} \\
& h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{23} + k_{332} = v_{32} + z_{32} + z_{33} + z_{42} \\
& h_{03} + h_{12} + h_{22} + h_{23} + h_{24} + k_{333} = v_{33} + z_{31} + z_{32} + z_{33} + z_{42} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{23} + k_{334} = v_{34} + \\
& z_{41} + z_{33} + z_{42} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{04} + h_{22} + h_{24} + k_{341} = v_{01} + v_{21} + z_{11} + \\
& z_{31} + z_{32} + z_{41} \\
& h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{23} + k_{342} = v_{02} + v_{22} + z_{12} + z_{32} + z_{33} + z_{42}
\end{aligned}$$

$$\begin{aligned}
& h_{03} + h_{12} + h_{22} + h_{23} + h_{24} + k_{343} = v_{03} + v_{23} + z_{13} + z_{31} + z_{32} + z_{33} + z_{42} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{23} + k_{344} = v_{04} + \\
& v_{24} + z_{14} + z_{41} + z_{33} + z_{42} + z_{44} \\
& k_{411} = v_{01} + v_{21} + v_{41} + z_{11} \\
& k_{412} = v_{02} + v_{22} + v_{42} + z_{12} \\
& k_{413} = v_{03} + v_{23} + v_{43} + z_{13} \\
& k_{414} = v_{04} + v_{24} + v_{44} + z_{14} \\
& h_{01} + h_{11} + h_{03} + h_{13} + h_{22} + h_{31} + h_{14} + h_{23} + h_{41} + h_{33} + k_{421} = \\
& v_{41} + z_{32} + z_{41} + z_{43} \\
& h_{11} + h_{31} + h_{23} + h_{32} + h_{24} + h_{42} + h_{34} + k_{422} = v_{42} + z_{41} \\
& h_{02} + h_{11} + h_{12} + h_{04} + h_{31} + h_{32} + h_{24} + h_{33} + h_{43} + k_{423} = v_{43} + z_{31} + z_{42} \\
& h_{02} + h_{12} + h_{21} + h_{13} + h_{22} + h_{32} + h_{34} + h_{44} + k_{424} = v_{44} + z_{31} + \\
& z_{32} + z_{41} + z_{42} + z_{34} + z_{43} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{12} + h_{21} + h_{13} + h_{14} + h_{32} + h_{34} + k_{431} = \\
& v_{41} + z_{31} + z_{42} + z_{34} + z_{43} + z_{44} \\
& h_{02} + h_{03} + h_{12} + h_{04} + h_{13} + h_{22} + h_{31} + h_{14} + h_{33} + k_{432} = v_{42} + \\
& z_{32} + z_{33} + z_{42} + z_{43} \\
& h_{01} + h_{02} + h_{03} + h_{04} + h_{13} + h_{22} + h_{32} + h_{33} + h_{34} + k_{433} = v_{43} + \\
& z_{31} + z_{32} + z_{43} + z_{44} \\
& h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{31} + h_{14} + h_{32} + h_{33} + h_{44} + k_{434} = \\
& v_{44} + z_{31} + z_{42} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{12} + h_{21} + h_{13} + h_{14} + h_{32} + h_{34} + k_{441} = \\
& v_{11} + v_{31} + z_{21} + z_{31} + z_{42} + z_{34} + z_{43} + z_{44} \\
& h_{02} + h_{03} + h_{12} + h_{04} + h_{13} + h_{22} + h_{31} + h_{14} + h_{33} + k_{442} = v_{12} + \\
& v_{32} + z_{22} + z_{32} + z_{33} + z_{42} + z_{43} \\
& h_{01} + h_{02} + h_{03} + h_{04} + h_{13} + h_{22} + h_{32} + h_{33} + h_{34} + k_{443} = v_{13} + \\
& v_{33} + z_{31} + z_{23} + z_{32} + z_{43} + z_{44} \\
& h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{31} + h_{14} + h_{32} + h_{24} + h_{33} + k_{444} = \\
& v_{14} + v_{34} + z_{31} + z_{24} + z_{42} + z_{44} \\
& h_{01} + h_{11} + h_{03} + h_{13} + h_{22} + h_{31} + h_{14} + h_{23} + h_{41} + h_{33} + k_{511} = \\
& v_{01} + v_{21} + v_{41} + v_{51} + z_{11} + z_{32} + z_{41} + z_{43} \\
& h_{11} + h_{31} + h_{23} + h_{32} + h_{24} + h_{42} + h_{34} + k_{512} = v_{02} + v_{22} + v_{42} + \\
& v_{52} + z_{12} + z_{41} \\
& h_{02} + h_{11} + h_{12} + h_{04} + h_{31} + h_{32} + h_{24} + h_{33} + h_{43} + k_{513} = v_{03} + \\
& v_{23} + v_{43} + v_{53} + z_{13} + z_{31} + z_{42} \\
& h_{02} + h_{12} + h_{21} + h_{13} + h_{22} + h_{32} + h_{34} + h_{44} + k_{514} = v_{04} + v_{24} + \\
& v_{44} + z_{31} + v_{54} + z_{14} + z_{32} + z_{41} + z_{42} + z_{34} + z_{43} \\
& h_{02} + h_{11} + h_{12} + h_{21} + h_{13} + h_{22} + h_{31} + h_{23} + h_{24} + k_{521} = v_{51} + \\
& z_{31} + z_{32} + z_{42} + z_{34} + z_{43}
\end{aligned}$$

$$\begin{aligned}
& h_{01} + h_{02} + h_{03} + h_{12} + h_{04} + h_{13} + h_{22} + h_{14} + h_{23} + h_{32} + h_{24} + k_{522} = \\
& v_{52} + z_{31} + z_{32} + z_{41} + z_{42} + z_{43} \\
& h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{14} + h_{24} + h_{33} + k_{523} = v_{53} + z_{31} + \\
& z_{41} + z_{42} + z_{34} \\
& h_{01} + h_{03} + h_{21} + h_{04} + h_{14} + h_{23} + h_{24} + h_{34} + k_{524} = v_{54} + z_{34} \\
& h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{33} + k_{531} = v_{51} + z_{32} + z_{42} + z_{34} \\
& h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + h_{34} + k_{532} = v_{52} + z_{32} + z_{33} + z_{42} + z_{34} \\
& h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + h_{31} + k_{533} = v_{53} + z_{33} + z_{34} + z_{43} \\
& h_{11} + h_{03} + h_{21} + h_{13} + h_{32} + h_{24} + z_{31} + k_{534} = v_{54} + z_{32} + z_{33} + z_{43} + z_{44} \\
& h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{14} + h_{33} + k_{541} = v_{11} + v_{31} + z_{21} + \\
& z_{32} + z_{42} + z_{34} \\
& h_{01} + h_{02} + h_{12} + h_{14} + h_{24} + h_{34} + k_{542} = v_{12} + v_{32} + z_{22} + z_{32} + z_{33} + \\
& z_{42} + z_{34} \\
& h_{02} + h_{11} + h_{03} + h_{21} + h_{13} + h_{31} + k_{543} = v_{13} + v_{33} + z_{23} + z_{33} + z_{34} + z_{43} \\
& h_{11} + h_{03} + h_{21} + h_{13} + h_{32} + h_{24} + k_{544} = v_{14} + v_{34} + z_{31} + z_{32} + z_{24} + \\
& z_{33} + z_{43} + z_{44} \\
& h_{01} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{31} + h_{23} + k_{611} = v_{11} + v_{31} + \\
& v_{61} + z_{21} + z_{41} + z_{42} + z_{34} + z_{43} \\
& h_{01} + h_{21} + h_{13} + h_{22} + h_{14} + h_{32} + h_{24} + k_{612} = v_{12} + v_{32} + v_{62} + \\
& z_{22} + z_{31} + z_{41} + z_{33} + z_{43} \\
& h_{01} + h_{02} + h_{21} + h_{22} + h_{14} + h_{23} + h_{33} + k_{613} = v_{13} + v_{33} + v_{63} + \\
& z_{23} + z_{32} + z_{41} + z_{33} + z_{34} \\
& h_{02} + h_{11} + h_{03} + h_{12} + h_{22} + h_{24} + h_{34} + k_{614} = v_{14} + v_{34} + z_{41} + \\
& v_{64} + z_{24} + z_{33} + z_{42} + z_{34} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{12} + h_{21} + h_{13} + h_{14} + k_{621} = v_{61} + z_{31} + \\
& z_{42} + z_{34} + z_{43} + z_{44} \\
& h_{02} + h_{03} + h_{12} + h_{04} + h_{13} + h_{22} + h_{14} + k_{622} = v_{62} + z_{32} + z_{33} + z_{42} + z_{43} \\
& h_{02} + h_{11} + h_{04} + h_{14} + h_{23} + z_{31} + k_{623} = v_{63} + z_{41} + z_{44} \\
& h_{11} + h_{04} + h_{13} + h_{14} + h_{24} + z_{32} + z_{41} + k_{624} = v_{64} + z_{34} + z_{43} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{04} + h_{23} + k_{631} = v_{61} + z_{41} + z_{33} + z_{42} \\
& h_{02} + h_{04} + h_{14} + h_{24} + k_{632} = v_{62} + z_{31} + z_{44} \\
& h_{01} + h_{11} + h_{03} + h_{21} + k_{633} = v_{63} + z_{32} + z_{41} \\
& h_{01} + h_{11} + h_{03} + h_{22} + h_{14} + z_{32} + z_{41} + k_{634} = v_{64} + z_{44} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{04} + h_{23} + k_{641} = v_{01} + v_{21} + v_{41} + v_{51} + z_{11} + \\
& z_{41} + z_{33} + z_{42} \\
& h_{02} + h_{04} + h_{14} + h_{24} + k_{642} = v_{02} + v_{22} + v_{42} + v_{52} + z_{12} + z_{31} + z_{44} \\
& h_{01} + h_{11} + h_{03} + h_{21} + k_{643} = v_{03} + v_{23} + v_{43} + v_{53} + z_{13} + z_{32} + z_{41} \\
& h_{01} + h_{11} + h_{03} + h_{22} + h_{14} + k_{644} = v_{04} + v_{24} + v_{44} + v_{54} + z_{14} + z_{32} + \\
& z_{41} + z_{44}
\end{aligned}$$

$$\begin{aligned}
 h02 + h11 + h03 + h21 + h13 + k7_{11} &= v01 + v21 + v41 + v51 + z11 + v71 + \\
 z33 + z34 + z43 & \\
 h11 + h03 + h12 + h04 + h22 + h14 + k7_{12} &= v02 + v22 + v42 + v52 + z12 + \\
 z31 + v72 + z41 + z33 + z42 + z34 & \\
 h11 + h12 + h04 + h13 + h23 + k7_{13} &= v03 + v23 + v43 + v53 + z13 + z32 + \\
 v73 + z42 + z34 + z43 & \\
 h01 + h02 + h12 + h14 + h24 + k7_{14} &= v04 + v24 + v44 + v54 + z14 + z32 + \\
 z33 + z42 + v74 + z34 & \\
 h01 + h02 + h11 + h03 + h04 + k7_{21} &= v71 + z31 + z32 + z41 \\
 h02 + h03 + h12 + h04 + k7_{22} &= v72 + z32 + z33 + z42 \\
 h01 + h04 + h13 + z31 + z32 + z41 + k7_{23} &= v73 + z33 + z34 + z43 \\
 h01 + h03 + h04 + h14 + k7_{24} &= v74 + z34
 \end{aligned}$$

## 【0063】

次に、ステップS104の行列方程式変換処理を実行する。ここで、ベクトルK, H, U, Vを下記のように設定する。

## 【0064】

## 【数16】

$$\begin{aligned}
 K &= (k_{111}, k_{112}, \dots, k_{724}) \\
 H &= (h_{01}, h_{02}, \dots, h_{44}) \\
 U &= (z_{11}, z_{12}, \dots, z_{44}) \\
 V &= (v_{01}, v_{02}, \dots, v_{74})
 \end{aligned}$$

## 【0065】

上記式のように、ベクトルK, H, U, Vを設定すると、上記連立線形方程式は以下のように行列方程式に変換できる。

## 【0066】

## 【数17】

$$M_{KH} \begin{pmatrix} {}^t\mathbf{K} \\ {}^t\mathbf{H} \end{pmatrix} = M_{UV} \begin{pmatrix} {}^t\mathbf{U} \\ {}^t\mathbf{V} \end{pmatrix}$$

## 【0067】

なお、上記式において、 $M_{KH}$ ,  $M_{UV}$ は、上記連立線形方程式の係数から成るGF(2)上の行列である。

## 【0068】

次に、ステップS105のユニタリ変換処理を実行する。

【0069】

【数18】

$$\text{rank } (M_{UV}) = N_r$$

【0070】

とする。また、行列 $M_{UV}$ の行数を $N_m$ とする。上記行列方程式の両辺に左から行変形ユニタリー行列 $Q$ を乗ずることによって、行列 $M_{UV}$ を階段行列に変形することができる。このとき、 $QM_{UV}$ のうち、下 $N_m - N_r$ 行から成る小行列は零行列になる。

【0071】

次に、ステップS106の小行列選択処理を実行する。 $QM_{KH}$ の下 $N_m - N_r$ 行の小行列を $M^*_{KH}$ とおくと、 $M^*_{KH}$ はゼロ行列(○)であり、下記式によって示される。

【0072】

【数19】

$$M^*_{KH} = \text{O}$$

【0073】

次にステップS107の線形関係式生成処理を実行する。この行列方程式を行毎の線形関係式に変換し、 $h01, h02, \dots, h44$ の具体的な値を代入すると、以下のような関係式が得られる。

【0074】

【数20】

$$\begin{aligned} 0xc7 &= k1_{11} + k1_{21} + k1_{22} + k1_{24} + k1_{31} + k1_{32} + k1_{34} + k1_{42} + k1_{44} + \\ &k2_{12} + k2_{14} + k2_{22} + k2_{24} + k2_{41} \\ 0x33 &= k1_{12} + k1_{21} + k1_{22} + k1_{23} + k1_{31} + k1_{32} + k1_{33} + k1_{41} + k1_{43} + \\ &k2_{11} + k2_{13} + k2_{21} + k2_{23} + k2_{42} \end{aligned}$$

$0x48 = k_{13} + k_{122} + k_{124} + k_{132} + k_{134} + k_{141} + k_{142} + k_{144} + k_{211} + k_{212} + k_{214} + k_{221} + k_{222} + k_{224} + k_{243}$   
 $0xef = k_{14} + k_{121} + k_{122} + k_{123} + k_{124} + k_{131} + k_{132} + k_{133} + k_{134} + k_{141} + k_{143} + k_{144} + k_{211} + k_{213} + k_{214} + k_{221} + k_{223} + k_{224} + k_{244}$   
 $0xc7 = k_{121} + k_{131} + k_{211} + k_{341}$   
 $0x33 = k_{122} + k_{132} + k_{212} + k_{342}$   
 $0x00 = k_{123} + k_{133} + k_{141} + k_{212} + k_{213} + k_{221} + k_{341} + k_{342} + k_{343}$   
 $0xd4 = k_{124} + k_{134} + k_{143} + k_{211} + k_{212} + k_{213} + k_{223} + k_{342} + k_{411} + k_{421}$   
 $0xc7 = k_{141} + k_{142} + k_{221} + k_{222} + k_{342} + k_{343} + k_{411} + k_{413} + k_{421} + k_{423}$   
 $0x74 = k_{142} + k_{143} + k_{211} + k_{212} + k_{222} + k_{223} + k_{342} + k_{343} + k_{411} + k_{412} + k_{421} + k_{422}$   
 $0x65 = k_{143} + k_{212} + k_{214} + k_{223} + k_{342} + k_{413} + k_{414} + k_{423} + k_{424}$   
 $0x33 = k_{144} + k_{211} + k_{224} + k_{341} + k_{344}$   
 $0x8a = k_{211} + k_{212} + k_{342} + k_{344} + k_{411} + k_{414} + k_{424} + k_{431}$   
 $0xf7 = k_{212} + k_{213} + k_{341} + k_{343} + k_{411} + k_{412} + k_{421} + k_{432}$   
 $0x29 = k_{213} + k_{214} + k_{341} + k_{342} + k_{344} + k_{411} + k_{412} + k_{413} + k_{421} + k_{422} + k_{433}$   
 $0xa1 = k_{214} + k_{341} + k_{344} + k_{411} + k_{422} + k_{423} + k_{424} + k_{431} + k_{432} + k_{433} + k_{434}$   
 $0x41 = k_{221} + k_{231} + k_{341} + k_{343} + k_{344} + k_{411} + k_{413} + k_{414} + k_{423} + k_{431} + k_{434}$   
 $0x74 = k_{222} + k_{232} + k_{341} + k_{342} + k_{343} + k_{411} + k_{412} + k_{413} + k_{423} + k_{424} + k_{431} + k_{432} + k_{434}$   
 $0xf4 = k_{223} + k_{233} + k_{341} + k_{342} + k_{343} + k_{344} + k_{411} + k_{412} + k_{413} + k_{414} + k_{424} + k_{431} + k_{432} + k_{433}$   
 $0x57 = k_{224} + k_{234} + k_{424} + k_{434}$   
 $0xf6 = k_{241} + k_{311} + k_{321} + k_{341} + k_{342} + k_{343} + k_{411} + k_{412} + k_{413} + k_{421} + k_{423} + k_{424} + k_{432} + k_{434}$   
 $0x7c = k_{242} + k_{312} + k_{322} + k_{342} + k_{412} + k_{422} + k_{423} + k_{424} + k_{433} + k_{434}$   
 $0x43 = k_{243} + k_{313} + k_{323} + k_{341} + k_{342} + k_{343} + k_{411} + k_{412} + k_{413} + k_{421} + k_{432} + k_{433}$   
 $0x5f = k_{244} + k_{314} + k_{324} + k_{343} + k_{413} + k_{422} + k_{424} + k_{432} + k_{433} + k_{434}$   
 $0x7d = k_{311} + k_{341} + k_{342} + k_{343} + k_{344} + k_{411} + k_{412} + k_{413} + k_{414} + k_{421} + k_{424} + k_{432} + k_{433} + k_{541}$   
 $0x2b = k_{312} + k_{341} + k_{342} + k_{411} + k_{412} + k_{422} + k_{423} + k_{431} + k_{433} + k_{542}$   
 $0x02 = k_{313} + k_{344} + k_{414} + k_{421} + k_{423} + k_{431} + k_{433} + k_{434} + k_{543}$   
 $0xde = k_{314} + k_{342} + k_{343} + k_{344} + k_{412} + k_{413} + k_{414} + k_{422} + k_{433} + k_{434} + k_{544}$

$0x8a = k3_{21} + k3_{31} + k3_{42} + k3_{43} + k3_{44} + k4_{12} + k4_{13} + k4_{14} + k4_{24} + k4_{32} + k4_{33}$   
 $0x7f = k3_{22} + k3_{32} + k3_{41} + k3_{42} + k3_{43} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{23} + k4_{24} + k4_{31} + k4_{32}$   
 $0x88 = k3_{23} + k3_{33} + k3_{41} + k3_{42} + k4_{11} + k4_{12} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{33} + k4_{34}$   
 $0x54 = k3_{24} + k3_{34} + k3_{42} + k3_{43} + k4_{12} + k4_{13} + k4_{22} + k4_{24} + k4_{33} + k4_{34}$   
 $0x7f = k3_{41} + k3_{42} + k4_{12} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{33} + k4_{34} + k5_{11} + k5_{21}$   
 $0x7f = k3_{42} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{24} + k4_{31} + k4_{32} + k4_{34} + k5_{11} + k5_{13} + k5_{21} + k5_{23}$   
 $0x8a = k3_{43} + k3_{44} + k4_{11} + k4_{13} + k4_{21} + k4_{31} + k4_{33} + k4_{34} + k5_{11} + k5_{14} + k5_{21} + k5_{24}$   
 $0x00 = k3_{44} + k4_{12} + k4_{14} + k4_{22} + k4_{32} + k4_{34} + k5_{12} + k5_{22}$   
 $0xf7 = k4_{11} + k4_{13} + k4_{23} + k4_{33} + k4_{41} + k5_{11} + k5_{13} + k5_{21} + k5_{23} + k5_{41}$   
 $0x29 = k4_{12} + k4_{13} + k4_{14} + k4_{21} + k4_{23} + k4_{24} + k4_{31} + k4_{33} + k4_{34} + k4_{41} + k4_{42} + k5_{12} + k5_{13} + k5_{14} + k5_{22} + k5_{23} + k5_{24} + k5_{41} + k5_{42}$   
 $0x2b = k4_{13} + k4_{14} + k4_{22} + k4_{24} + k4_{32} + k4_{34} + k4_{42} + k4_{43} + k5_{13} + k5_{14} + k5_{23} + k5_{24} + k5_{42} + k5_{43}$   
 $0x88 = k4_{14} + k4_{21} + k4_{23} + k4_{31} + k4_{33} + k4_{41} + k4_{43} + k4_{44} + k5_{14} + k5_{24} + k5_{41} + k5_{43} + k5_{44}$   
 $0x43 = k4_{21} + k4_{31} + k5_{41} + k6_{11} + k6_{21}$   
 $0xc0 = k4_{22} + k4_{24} + k4_{32} + k4_{34} + k4_{41} + k4_{42} + k4_{44} + k5_{44} + k6_{11} + k6_{12} + k6_{21} + k6_{32}$   
 $0xcb = k4_{23} + k4_{24} + k4_{33} + k4_{34} + k4_{41} + k5_{43} + k6_{11} + k6_{13} + k6_{21} + k6_{33}$   
 $0x81 = k4_{24} + k4_{34} + k4_{42} + k4_{43} + k5_{43} + k6_{12} + k6_{22}$   
 $0x7e = k4_{41} + k5_{41} + k5_{43} + k6_{13} + k6_{23}$   
 $0xdd = k4_{42} + k4_{43} + k4_{44} + k5_{42} + k5_{43} + k6_{14} + k6_{24}$   
 $0x00 = k4_{43} + k4_{44} + k5_{43} + k6_{14} + k6_{34}$   
 $0x00 = k4_{44} + k5_{41} + k5_{44} + k6_{11} + k6_{31}$   
 $0xf7 = k5_{11} + k5_{41} + k6_{11} + k6_{31} + k6_{41}$   
 $0x14 = k5_{12} + k5_{41} + k5_{43} + k5_{44} + k6_{11} + k6_{13} + k6_{14} + k6_{21} + k6_{23} + k6_{34} + k6_{42}$   
 $0x23 = k5_{13} + k5_{41} + k5_{42} + k6_{11} + k6_{12} + k6_{22} + k6_{24} + k6_{31} + k6_{34} + k6_{43}$   
 $0x8a = k5_{14} + k5_{44} + k6_{14} + k6_{34} + k6_{44}$   
 $0xb4 = k5_{21} + k5_{31} + k5_{41} + k5_{42} + k6_{11} + k6_{12} + k6_{21} + k6_{32}$   
 $0x0b = k5_{22} + k5_{32} + k5_{42} + k5_{43} + k6_{12} + k6_{13} + k6_{22} + k6_{33}$   
 $0x00 = k5_{23} + k5_{33} + k5_{41} + k5_{42} + k5_{44} + k6_{11} + k6_{12} + k6_{14} + k6_{31} + k6_{32} + k6_{34}$

$$\begin{aligned}
 0x00 &= k_{524} + k_{534} + k_{541} + k_{543} + k_{544} + k_{611} + k_{613} + k_{614} + k_{631} + \\
 &k_{633} + k_{634} \\
 0xc7 &= k_{541} + k_{542} + k_{543} + k_{544} + k_{611} + k_{612} + k_{613} + k_{614} + k_{621} + \\
 &k_{623} + k_{632} + k_{634} + k_{641} + k_{711} + k_{721} \\
 0xfc &= k_{542} + k_{612} + k_{621} + k_{631} + k_{632} + k_{643} + k_{713} + k_{723} \\
 0x18 &= k_{543} + k_{544} + k_{613} + k_{614} + k_{621} + k_{622} + k_{631} + k_{632} + k_{633} + \\
 &k_{634} + k_{643} + k_{644} + k_{713} + k_{714} + k_{723} + k_{724} \\
 0xf4 &= k_{621} + k_{622} + k_{623} + k_{624} + k_{631} + k_{632} + k_{633} + k_{634} + k_{641} + \\
 &k_{642} + k_{711} + k_{712} + k_{721} + k_{722}
 \end{aligned}$$

## 【0075】

ここで、下記式が成立する。

## 【0076】

## 【数21】

$$\text{rank } (M^*_{KH}) = N_m - N_r$$

## 【0077】

従って、上記60個の線形関係式は、互いに独立な線形関係式である。従って、これら60個のGF(2)上の任意を線形結合して得られる $2^{60}-1$ 個の線形関係式が成り立つことがわかる。この線形関係式が多ければ、暗号の設計者の意図しない新たな攻撃を招く恐れがあるので、上述した方法によって得られた線形関係式の総数を、暗号強度評価の一つの指標として用いることができる。

## 【0078】

## 【暗号強度指標算出処理具体例2】

次に、本発明に係る暗号強度指標算出処理の第2の具体例として、東芝から提案されたブロック暗号「Hierocrypt-3」に対して本発明に係る暗号強度評価方法を適用した処理例の詳細について説明する。Hierocrypt-3は、AES互換の暗号であり、ブロック長は128bit、鍵長は、128,192,256の何れかである。以下に説明する処理例は、鍵長が256bitである場合についての処理例である。

## 【0079】

まず、図1に示すステップS101の暗号処理アルゴリズムの設定ステップについて説明する。ここでは、東芝から提案されたブロック暗号「Hierocrypt-3」の設定処理として実行する。

## 【0080】

まず、行列P32は以下のように定義される。

【0081】

【数22】

$$P32 = \begin{pmatrix} I_4 & O_4 & I_4 & O_4 \\ O_4 & I_4 & O_4 & I_4 \\ O_4 & I_4 & I_4 & I_4 \\ I_4 & O_4 & I_4 & I_4 \end{pmatrix}$$

【0082】

また、行列P32Iを、行列P32の逆行列とする。次に、行列M51、M52、MB1、MB2を以下のように定義する。

【0083】

【数23】

$$M51 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$M52 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$MB1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$MB2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

【0084】

さらに、行列M51、M52、MB1、MB2を用いて、以下のように行列M5、MBを定義する。

【0085】

## 【数24】

$$M5 = \begin{pmatrix} M51 & O4 & O4 & O4 \\ O4 & M52 & O4 & O4 \\ O4 & O4 & M51 & O4 \\ O4 & O4 & O4 & M52 \end{pmatrix}$$

$$MB = \begin{pmatrix} MB1 & O4 & O4 & O4 \\ O4 & MB2 & O4 & O4 \\ O4 & O4 & MB1 & O4 \\ O4 & O4 & O4 & MB2 \end{pmatrix}$$

## 【0086】

次に、ラウンド依存定数ベクトル  $G_i$  ( $(i = 0, \dots, 9)$ ) を以下のように定義する。

## 【0087】

## 【数25】

$$G0 = (h11, h12, h13, h14, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G1 = (h21, h22, h23, h24, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G2 = (h31, h32, h33, h34, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G3 = (h11, h12, h13, h14, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G4 = (h21, h22, h23, h24, h11, h12, h13, h14, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G5 = (h01, h02, h03, h04, h21, h22, h23, h24, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G6 = (h01, h02, h03, h04, h21, h22, h23, h24, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G7 = (h21, h22, h23, h24, h11, h12, h13, h14, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G8 = (h11, h12, h13, h14, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$G9 = (h31, h32, h33, h34, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

## 【0088】

なお、上式で用いられている定数を要素とするベクトル  $HH$  は、先に【暗号強度指標算出処理具体例2】において説明したと同一である。

## 【0089】

次に、鍵スケジュール部の初期値の右半分から成るベクトル  $ZZ$  を、以下のように定義する。

## 【0090】

## 【数26】

$ZZ = (z_{31}, z_{32}, z_{33}, z_{34}, z_{35}, z_{36}, z_{37}, z_{38}, z_{41}, z_{42}, z_{43}, z_{44}, z_{45}, z_{46}, z_{47}, z_{48})$

## 【0091】

これらを用いて、共通鍵暗号アルゴリズムHierocrypt-3の鍵スケジュール部の右半分は、以下のように表せる。なお、演算子 $+$ は、ガロア体GF(2)上の加法演算子である。

## 【0092】

## 【数27】

$$Z_0 M_5 * Z_Z + G_0$$

$$W_0 = P_3 2 * Z_0$$

$$Z_1 = M_5 * W_0 + G_1$$

$$W_1 = P_3 2 * Z_1$$

$$Z_2 = M_5 * W_1 + G_2$$

$$W_2 = P_3 2 * Z_2$$

$$Z_3 = M_5 * W_2 + G_3$$

$$W_3 = P_3 2 * Z_3$$

$$Z_4 = M_5 * W_3 + G_4$$

$$W_4 = P_3 2 * Z_4$$

$$Z_5 = M_5 * W_4 + G_5$$

$$W_6 = MB * (Z_5 + G_6)$$

$$Z_6 = P_3 2 I * W_6$$

$$W_7 = MB * (Z_6 + G_7)$$

$$Z_7 = P_3 2 I * W_7$$

$$W_8 = MB * (Z_7 + G_8)$$

$$Z_8 = P_3 2 I * W_8$$

$$W_9 = MB * (Z_8 + G_9)$$

$$Z_9 = P_3 2 I * W_9$$

## 【0093】

ここで、 $Z_0, Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8, Z_9, W_0, W_1, W_2, W_3, W_5, W_6, W_7, W_8, W_9$ は、鍵スケジュール部の中間値の右半分を表す。

【0094】

次に、これらの中間値を、下式、

【0095】

【数28】

$$Z_n = Z_{n_3} || Z_{N_4}$$

$$W_n = W_{n_1} || W_{N_2}$$

【0096】

のように分割して表現する。但し記号“||”は、ベクトルの連結を表す。

【0097】

次に、各ラウンドの非線形変換部出力を、V0,V1,V2,V3,V4,V5,V6,V7,V8,V9とする。

但し、各々は、下記に示す8つの要素から成るベクトルである。

【0098】

【数29】

$$V0 = (v01, v02, v03, v04, v05, v06, v07, v08)$$

$$V1 = (v11, v12, v13, v14, v15, v16, v17, v18)$$

$$V2 = (v21, v22, v23, v24, v25, v26, v27, v28)$$

$$V3 = (v31, v32, v33, v34, v35, v36, v37, v38)$$

$$V4 = (v41, v42, v43, v44, v45, v46, v47, v48)$$

$$V5 = (v51, v52, v53, v54, v55, v56, v57, v58)$$

$$V6 = (v61, v62, v63, v64, v65, v66, v67, v68)$$

$$V7 = (v71, v72, v73, v74, v75, v76, v77, v78)$$

$$V8 = (v81, v82, v83, v84, v85, v86, v87, v88)$$

$$V9 = (v91, v92, v93, v94, v95, v96, v97, v98)$$

【0099】

ここで、ベクトル $Z_1$ 、 $Z_2$ を下記のように設定する。

【0100】

【数30】

$$Z_1 = (z11, z12, z13, z14, z15, z16, z17, z18)$$

$Z_2 = (z_{21}, z_{22}, z_{23}, z_{24}, z_{25}, z_{26}, z_{27}, z_{28})$

【0101】

上記のように、ベクトル  $Z_1$ 、 $Z_2$  を設定すると、Hierocrypt-3 の鍵スケジュール部の左半分は、以下のように表せる。

【0102】

【数31】

$$Z_{01} = Z_2$$

$$Z_{02} = Z_1 + V_0$$

$$Z_{11} = Z_{02}$$

$$Z_{12} = Z_{01} + V_1$$

$$Z_{21} = Z_{12}$$

$$Z_{22} = Z_{11} + V_2$$

$$Z_{31} = Z_{22}$$

$$Z_{32} = Z_{21} + V_3$$

$$Z_{41} = Z_{32}$$

$$Z_{42} = Z_{31} + V_4$$

$$Z_{51} = Z_{42}$$

$$Z_{52} = Z_{41} + V_5$$

$$Z_{61} = Z_{52} + V_6$$

$$Z_{62} = Z_{51}$$

$$Z_{71} = Z_{62} + V_7$$

$$Z_{72} = Z_{61}$$

$$Z_{81} = Z_{72} + V_8$$

$$Z_{82} = Z_{71}$$

$$Z_{91} = Z_{82} + V_9$$

$$Z_{92} = Z_{81}$$

【0103】

ここで、 $Z_{01}$ 、 $Z_{02}$ 、 $Z_{11}$ 、 $Z_{12}$ 、 $Z_{21}$ 、 $Z_{22}$ 、 $Z_{31}$ 、 $Z_{32}$ 、 $Z_{41}$ 、 $Z_{42}$ 、 $Z_{51}$ 、 $Z_{52}$ 、 $Z_{61}$ 、 $Z_{62}$ 、 $Z_{71}$ 、 $Z_{72}$ 、 $Z_{81}$ 、 $Z_{82}$ 、 $Z_{91}$ 、 $Z_{92}$ 、

$Z_{9_2}$ は、鍵スケジュール部の中間値の左半分を表す。こうして得られた中間値を用いて、ラウンド鍵 $K_{1_1}, K_{1_2}, K_{1_3}, K_{1_4}, K_{2_1}, \dots, K_{9_1}, K_{9_2}$ は、以下のように表せる。

【0104】

【数32】

$$K_{1_1} = Z_{0_1} + V_{1_1}$$

$$K_{1_2} = Z_{1_3} + V_{1_2}$$

$$K_{1_3} = Z_{1_4} + V_{1_3}$$

$$K_{1_4} = Z_{0_2} + Z_{1_4}$$

$$K_{2_1} = Z_{1_1} + V_{2_1}$$

$$K_{2_2} = Z_{2_3} + V_{2_2}$$

$$K_{2_3} = Z_{2_4} + V_{2_3}$$

$$K_{2_4} = Z_{1_2} + Z_{2_4}$$

$$K_{3_1} = Z_{2_1} + V_{3_1}$$

$$K_{3_2} = Z_{3_3} + V_{3_2}$$

$$K_{3_3} = Z_{3_4} + V_{3_3}$$

$$K_{3_4} = Z_{2_2} + Z_{3_4}$$

$$K_{4_1} = Z_{3_1} + V_{4_1}$$

$$K_{4_2} = Z_{4_3} + V_{4_2}$$

$$K_{4_3} = Z_{4_4} + V_{4_3}$$

$$K_{4_4} = Z_{3_2} + Z_{4_4}$$

$$K_{5_1} = Z_{4_1} + V_{5_1}$$

$$K_{5_2} = Z_{5_3} + V_{5_2}$$

$$K_{5_3} = Z_{5_4} + V_{5_3}$$

$$K_{5_4} = Z_{4_2} + Z_{5_4}$$

$$K_{6_1} = Z_{6_1} + Z_{5_3}$$

$$K_{6_2} = W_{6_1} + V_{6_2}$$

$$K_{6_3} = W_{6_2} + V_{6_3}$$

$$K_{6_4} = Z_{5_1} + W_{6_2}$$

$$K7_1 = Z7_1 + Z6_3$$

$$K7_2 = W7_1 + V7$$

$$K7_3 = W7_2 + V7$$

$$K7_4 = Z6_1 + W7_2$$

$$K8_1 = Z8_1 + Z7_3$$

$$K8_2 = W8_1 + V8$$

$$K8_3 = W8_2 + V8$$

$$K8_4 = Z7_1 + W8_2$$

$$K9_1 = Z9_1 + Z8_3$$

$$K9_2 = W9_1 + V9$$

$$K9_3 = W9_2 + V9$$

$$K9_4 = Z8_1 + W9_2$$

【0105】

なお、 $K1_1, K1_2, K1_3, K1_4, K2_1, \dots, K9_1, K9_2$ は、8つの要素成るベクトルである。

【0106】

次に、図1に示すステップS102の中間変数消去処理ステップについて説明する。上述の8つの要素から成るベクトル $K1_1, K1_2, K1_3, K1_4, K2_1, \dots, K9_1, K9_2$ について、実際に各値を代入して計算すると、以下のような式が得られる。

【0107】

【数 3 3】

$$\begin{aligned}
 K_{1_1} &= \begin{pmatrix} v11 + z21 \\ v12 + z22 \\ v13 + z23 \\ v14 + z24 \\ v15 + z25 \\ v16 + z26 \\ v17 + z27 \\ v18 + z28 \end{pmatrix} \\
 K_{1_2} &= \begin{pmatrix} h11 + h21 + h13 + v11 + z32 + z42 \\ h11 + h12 + h22 + h14 + v12 + z33 + z43 \\ h11 + h12 + h13 + h23 + v13 + z31 + z41 + z34 + z44 \\ h12 + h14 + h24 + v14 + z31 + z41 \\ h01 + h02 + h03 + h04 + h31 + v15 + z36 + z46 + z38 + z48 \\ h02 + h03 + h04 + h32 + v16 + z35 + z45 + z37 + z47 \\ h03 + h04 + h33 + v17 + z35 + z36 + z45 + z46 + z38 + z48 \\ h01 + h02 + h03 + h34 + v18 + z35 + z45 + z37 + z38 + z47 + z48 \end{pmatrix}
 \end{aligned}$$

$$\begin{aligned}
K_{13} &= \left( \begin{array}{l} h01 + h03 + v11 + z42 + z35 + z36 + z45 + z46 \\ h01 + h02 + h04 + v12 + z43 + z36 + z37 + z46 + z47 \\ h01 + h02 + h03 + v13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48 \\ h02 + h04 + v14 + z41 + z35 + z45 + z38 + z48 \\ h11 + h12 + h13 + h14 + v15 + z31 + z32 + z41 + z42 + z46 + z48 \\ h12 + h13 + h14 + v16 + z32 + z33 + z42 + z43 + z45 + z47 \\ h13 + h14 + v17 + z31 + z41 + z33 + z34 + z43 + z44 + z45 + z46 + z48 \\ h11 + h12 + h13 + z31 + v18 + z41 + z34 + z44 + z45 + z47 + z48 \end{array} \right) \\
K_{14} &= \left( \begin{array}{l} h01 + h03 + v01 + z11 + z42 + z35 + z36 + z45 + z46 \\ h01 + h02 + h04 + v02 + z12 + z43 + z36 + z37 + z46 + z47 \\ h01 + h02 + h03 + v03 + z13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48 \\ h02 + h04 + v04 + z14 + z41 + z35 + z45 + z38 + z48 \\ h11 + h12 + h13 + h14 + v05 + z31 + z32 + z41 + z15 + z42 + z46 + z48 \\ h12 + h13 + h14 + v06 + z32 + z33 + z42 + z16 + z43 + z45 + z47 \\ h13 + h14 + v07 + z31 + z41 + z33 + z34 + z43 + z17 + z44 + z45 + z46 + z48 \\ h11 + h12 + h13 + v08 + z31 + z41 + z34 + z44 + z18 + z45 + z47 + z48 \end{array} \right) \\
K_{21} &= \left( \begin{array}{l} v01 + v21 + z11 \\ v02 + v22 + z12 \\ v03 + v23 + z13 \\ v04 + v24 + z14 \\ v05 + v25 + z15 \\ v06 + v26 + z16 \\ v07 + v27 + z17 \\ v08 + v28 + z18 \end{array} \right) \\
K_{22} &= \left( \begin{array}{l} h02 + h12 + h21 + h31 + h23 + v21 + z31 + z32 + z34 + z36 + z37 + z46 + z38 \\ +z47 + z48 \\ h03 + h21 + h13 + h22 + h32 + h24 + v22 + z31 + z32 + z33 + z37 + z38 + z47 \\ +z48 \\ h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + v23 + z31 + z32 + z33 + z34 \\ +z38 + z48 \\ h01 + h11 + h22 + h24 + h34 + v24 + z31 + z33 + z35 + z36 + z45 + z37 + z46 \\ +z38 + z47 + z48 \\ h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + v25 + z31 + z41 + z35 \\ +z38 \\ h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + v26 + z32 + z42 + z35 + z36 \\ h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + v27 + z33 + z43 + z36 \\ +z37 \\ h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + v28 + z34 + z44 + z37 \end{array} \right)
\end{aligned}$$

$$\begin{aligned}
K_{2_3} = & \left( \begin{array}{l} h01 + h11 + h12 + h31 + h33 + v21 + z32 + z41 + z33 + z34 + z43 + z35 + z36 \\ + z37 + z46 + z38 + z47 + z48 \\ h02 + h12 + h13 + h31 + h32 + h34 + v22 + z41 + z33 + z42 + z34 + z44 + z36 \\ + z37 + z38 + z47 + z48 \\ h11 + h03 + h13 + h31 + h14 + h32 + h33 + v23 + z41 + z42 + z34 + z43 + z37 \\ + z38 + z48 \\ h11 + h04 + h14 + h32 + h34 + v24 + z31 + z32 + z33 + z42 + z34 + z35 + z44 \\ + z36 + z45 + z37 + z46 + z47 + z48 \\ h01 + h02 + h11 + h21 + h22 + h14 + h23 + h24 + v25 + z31 + z32 + z41 + z33 \\ + z34 + z35 + z48 \\ h02 + h11 + h03 + h12 + h22 + h23 + h24 + v26 + z32 + z33 + z42 + z34 + z36 \\ + z45 \\ h01 + h03 + h12 + h04 + h13 + h23 + h24 + v27 + z33 + z34 + z43 + z37 + z46 \\ h01 + h21 + h04 + h13 + h22 + h23 + z31 + z32 + v28 + z33 + z44 + z38 + z47 \\ + z48 \end{array} \right) \\
K_{2_4} = & \left( \begin{array}{l} h01 + h11 + h12 + h31 + h33 + v11 + z21 + z32 + z41 + z33 + z34 + z43 + z35 \\ + z36 + z37 + z46 + z38 + z47 + z48 \\ h02 + h12 + h13 + h31 + h32 + h34 + v12 + z22 + z41 + z33 + z42 + z34 + z44 \\ + z36 + z37 + z38 + z47 + z48 \\ h11 + h03 + h13 + h31 + h14 + h32 + h33 + v13 + z23 + z41 + z42 + z34 + z43 \\ + z37 + z38 + z48 \\ h11 + h04 + h14 + h32 + h34 + v14 + z31 + z32 + z24 + z33 + z42 + z34 + z35 \\ + z44 + z36 + z45 + z37 + z46 + z47 + z48 \\ h01 + h02 + h11 + h21 + h22 + h14 + h23 + h24 + v15 + z31 + z32 + z41 + z33 \\ + z25 + z34 + z35 + z48 \\ h02 + h11 + h03 + h12 + h22 + h23 + h24 + v16 + z32 + z33 + z42 + z34 + z26 \\ + z36 + z45 \\ h01 + h03 + h12 + h04 + h13 + h23 + h24 + v17 + z33 + z34 + z43 + z27 + z37 \\ + z46 \\ h01 + h21 + h04 + h13 + h22 + h23 + z31 + v18 + z32 + z33 + z44 + z28 + z38 \\ + z47 + z48 \end{array} \right) \\
K_{3_1} = & \left( \begin{array}{l} v11 + v31 + z21 \\ v12 + v32 + z22 \\ v13 + v33 + z23 \\ v14 + v34 + z24 \\ v15 + v35 + z25 \\ v16 + v36 + z26 \\ v17 + v37 + z27 \\ v18 + v38 + z28 \end{array} \right)
\end{aligned}$$

$$\begin{aligned}
K_{3_2} = & \left( \begin{array}{l}
h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + v31 + z32 + z42 + z35 + z37 \\
h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + v32 + z33 + z43 + z35 \\
+z36 + z38 \\
h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + v33 + z31 + z41 + z34 + z35 \\
+z44 + z36 + z37 \\
h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + v34 + z31 + z41 + z36 \\
+z38 \\
h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + v35 + z31 + z33 + z35 \\
+z36 + z45 + z37 + z46 + z47 \\
h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + z31 + v36 + z32 \\
+z34 + z35 + z36 + z45 + z37 + z46 + z38 + z47 + z48 \\
h02 + h03 + h21 + h04 + h13 + h22 + h31 + h32 + h24 + h33 + h34 + z31 + z32 \\
+v37 + z33 + z36 + z37 + z46 + z38 + z47 + z48 \\
h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + z32 + v38 + z34 + z35 \\
+z36 + z45 + z46 + z38 + z48
\end{array} \right) \\
K_{3_3} = & \left( \begin{array}{l}
h01 + h02 + h03 + h21 + h04 + h22 + h31 + v31 + z42 + z35 + z38 + z47 + z48 \\
h02 + h03 + h04 + h22 + h23 + h32 + v32 + z43 + z35 + z36 + z48 \\
h03 + h21 + h04 + h23 + h24 + h33 + v33 + z41 + z44 + z36 + z45 + z37 \\
h01 + h02 + h03 + h21 + h24 + h34 + v34 + z41 + z37 + z46 + z47 + z48 \\
h11 + h12 + h21 + h13 + h24 + h33 + h34 + v35 + z31 + z34 + z43 + z44 + z45 \\
+z46 + z47 \\
h11 + h12 + h21 + h13 + h22 + h14 + h34 + z31 + v36 + z32 + z44 + z45 + z46 \\
+z47 + z48 \\
h12 + h13 + h22 + h31 + h14 + h23 + z32 + z41 + v37 + z33 + z46 + z47 + z48 \\
h11 + h12 + h14 + h23 + h32 + h33 + h34 + z33 + z42 + v38 + z43 + z44 + z45 \\
+z46 + z48
\end{array} \right)
\end{aligned}$$

$$\begin{aligned}
K_{34} &= \left( \begin{array}{l}
h01 + h02 + h03 + h21 + h04 + h22 + h31 + v01 + v21 + z11 + z42 + z35 + z38 \\
+z47 + z48 \\
h02 + h03 + h04 + h22 + h23 + h32 + v02 + v22 + z12 + z43 + z35 + z36 + z48 \\
h03 + h21 + h04 + h23 + h24 + h33 + v03 + v23 + z13 + z41 + z44 + z36 + z45 \\
+z37 \\
h01 + h02 + h03 + h21 + h24 + h34 + v04 + v24 + z14 + z41 + z37 + z46 + z47 \\
+z48 \\
h11 + h12 + h21 + h13 + h24 + h33 + h34 + v05 + v25 + z31 + z15 + z34 + z43 \\
+z44 + z45 + z46 + z47 \\
h11 + h12 + h21 + h13 + h22 + h14 + h34 + v06 + v26 + z31 + z32 + z16 + z44 \\
+z45 + z46 + z47 + z48 \\
h12 + h13 + h22 + h31 + h14 + h23 + v07 + v27 + z32 + z41 + z33 + z17 + z46 \\
+z47 + z48 \\
h11 + h12 + h14 + h23 + h32 + h33 + h34 + v08 + v28 + z33 + z42 + z43 + z44 \\
+z18 + z45 + z46 + z48 \\
v01 + v21 + v41 + z11 \\
v02 + v22 + v42 + z12 \\
v03 + v23 + v43 + z13 \\
v04 + v24 + v44 + z14 \\
v05 + v25 + v45 + z15 \\
v06 + v26 + v46 + z16 \\
v07 + v27 + v47 + z17 \\
v08 + v28 + v48 + z18
\end{array} \right) \\
K_{41} &= \left( \begin{array}{l}
h01 + h11 + h03 + h12 + h13 + h23 + h33 + h34 + v41 + z31 + z32 + z34 + z35 + z45 \\
+z37 + z38 + z47 + z48 \\
h01 + h02 + h11 + h12 + h21 + h04 + h13 + h14 + h24 + h34 + v42 + z31 + z32 + z33 \\
+z36 + z46 + z38 + z48 \\
h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h14 + v43 + z31 + z32 + z33 + z34 \\
+z35 + z45 + z37 + z47 \\
h02 + h11 + h12 + h04 + h22 + h14 + h32 + h33 + h34 + v44 + z31 + z33 + z36 + z37 \\
+z46 + z47 \\
h01 + h11 + h03 + h12 + h21 + h04 + h31 + h33 + h34 + z31 + v45 + z32 + z41 + z42 \\
+z34 + z35 + z44 + z37 + z38 \\
h02 + h12 + h04 + h13 + h22 + h32 + h34 + z31 + z32 + z41 + v46 + z33 + z42 + z43 \\
+z36 + z38 \\
h01 + h11 + h03 + h13 + h31 + h14 + h23 + h33 + z31 + z32 + z41 + z33 + z42 + v47 \\
+z34 + z43 + z35 + z44 + z37 \\
h02 + h11 + h03 + h14 + h32 + h24 + h33 + z31 + z41 + z33 + z43 + v48 + z36 + z37
\end{array} \right)
\end{aligned}$$

$$\begin{aligned}
& h02 + h04 + h13 + h14 + h33 + h34 + v41 + z31 + z33 + z42 + z34 + z43 + z36 + z45 \\
& + z37 + z47 + z48 \\
& h01 + h03 + h14 + h34 + v42 + z32 + z41 + z34 + z43 + z35 + z44 + z37 + z46 + z38 \\
& + z48 \\
& h01 + h02 + h11 + h04 + h31 + v43 + z31 + z33 + z42 + z44 + z36 + z45 + z38 + z47 \\
& h01 + h03 + h12 + h04 + h13 + h14 + h32 + h33 + h34 + v44 + z32 + z41 + z33 + z42 \\
& + z35 + z36 + z46 + z47 \\
K4_3 = & h01 + h02 + h11 + h03 + h21 + h04 + h22 + h31 + h23 + h34 + v45 + z32 + z41 + z33 \\
& + z42 + z35 + z44 + z36 + z46 + z38 + z47 \\
& h02 + h03 + h12 + h21 + h04 + h22 + h31 + h23 + h32 + h24 + z31 + z41 + v46 + z33 \\
& + z42 + z34 + z43 + z35 + z36 + z45 + z37 + z47 + z48 \\
& h03 + h04 + h13 + h22 + h23 + h32 + h24 + h33 + z32 + z41 + z42 + v47 + z34 + z43 \\
& + z35 + z44 + z36 + z37 + z46 + z38 + z48 \\
& h01 + h02 + h03 + h21 + h22 + h14 + h24 + h33 + z31 + z32 + z41 + z43 + v48 + z35 \\
& + z45 + z37 + z46 \\
& h02 + h04 + h13 + h14 + h33 + h34 + v11 + v31 + z21 + z31 + z33 + z42 + z34 + z43 \\
& + z36 + z45 + z37 + z47 + z48 \\
& h01 + h03 + h14 + h34 + v12 + v32 + z22 + z32 + z41 + z34 + z43 + z35 + z44 + z37 \\
& + z46 + z38 + z48 \\
& h01 + h02 + h11 + h04 + h31 + v13 + v33 + z31 + z23 + z33 + z42 + z44 + z36 + z45 \\
& + z38 + z47 \\
& h01 + h03 + h12 + h04 + h13 + h14 + h32 + h33 + h34 + v14 + v34 + z32 + z41 + z24 \\
& + z33 + z42 + z35 + z36 + z46 + z47 \\
K4_4 = & h01 + h02 + h11 + h03 + h21 + h04 + h22 + h31 + h23 + h34 + v15 + v35 + z32 + z41 \\
& + z33 + z42 + z25 + z35 + z44 + z36 + z46 + z38 + z47 \\
& h02 + h03 + h12 + h21 + h04 + h22 + h31 + h23 + h32 + h24 + v16 + z31 + v36 + z41 \\
& + z33 + z42 + z34 + z43 + z26 + z35 + z36 + z45 + z37 + z47 + z48 \\
& h03 + h04 + h13 + h22 + h23 + h32 + h24 + h33 + v17 + z32 + z41 + v37 + z42 + z34 \\
& + z43 + z35 + z44 + z27 + z36 + z37 + z46 + z38 + z48 \\
& h01 + h02 + h03 + h21 + h22 + h14 + h24 + h33 + z31 + v18 + z32 + z41 + v38 + z43 \\
& + z35 + z45 + z28 + z37 + z46 \\
& \left. \begin{array}{l} v11 + v31 + v51 + z21 \\ v12 + v32 + v52 + z22 \\ v13 + v33 + v53 + z23 \\ v14 + v34 + v54 + z24 \\ v15 + v35 + v55 + z25 \\ v16 + v36 + v56 + z26 \\ v17 + v37 + v57 + z27 \\ v18 + v38 + v58 + z28 \end{array} \right) \\
K5_1 = &
\end{aligned}$$

$$\begin{aligned}
K_{5_2} = & \left. \begin{array}{l} h02 + h21 + h13 + h22 + h23 + v51 + z33 + z34 + z43 + z44 + z37 \\ h11 + h03 + h21 + h22 + h14 + h23 + h24 + v52 + z34 + z35 + z44 + z38 \\ h01 + h11 + h12 + h04 + h22 + h23 + h24 + v53 + z31 + z41 + z35 + z36 \\ h01 + h12 + h21 + h22 + h24 + v54 + z32 + z33 + z42 + z34 + z43 + z44 + z36 \\ h02 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + v55 + z33 + z36 + z46 \\ h03 + h04 + h13 + h22 + h14 + h23 + h34 + z31 + v56 + z34 + z37 + z47 \\ h21 + h04 + h31 + h14 + h23 + h24 + z31 + z32 + v57 + z35 + z45 + z38 + z48 \\ h01 + h02 + h11 + h03 + h12 + h21 + h04 + h13 + h14 + h32 + h24 + h33 + h34 + z32 \\ + z35 + v58 + z45 \end{array} \right\} \\
K_{5_3} = & \left. \begin{array}{l} h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + v51 + z43 + z44 + z47 \\ h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + v52 + z44 + z45 + z48 \\ h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + v53 + z41 + z45 + z46 \\ h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + v54 + z42 + z43 \\ + z44 + z46 \\ h11 + h21 + h14 + h34 + v55 + z43 + z46 \\ h11 + h12 + h22 + h31 + z41 + v56 + z44 + z47 \\ h12 + h13 + h23 + h32 + z41 + z42 + v57 + z45 + z48 \\ h13 + h24 + h33 + h34 + z42 + v58 + z45 \end{array} \right\} \\
K_{5_4} = & \left. \begin{array}{l} h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + v01 + v21 + v41 + z11 + z43 \\ + z44 + z47 \\ h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + v02 + v22 + v42 + z12 + z44 \\ + z45 + z48 \\ h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + v03 + v23 + v43 + z13 \\ + z41 + z45 + z46 \\ h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + v04 + v24 \\ + v44 + z14 + z42 + z43 + z44 + z46 \\ h11 + h21 + h14 + h34 + v05 + v25 + v45 + z15 + z43 + z46 \\ h11 + h12 + h22 + h31 + v06 + v26 + z41 + v46 + z16 + z44 + z47 \\ h12 + h13 + h23 + h32 + v07 + v27 + z41 + z42 + v47 + z17 + z45 + z48 \\ h13 + h24 + h33 + h34 + v08 + v28 + z42 + v48 + z18 + z45 \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
K_{6_1} = & \left. \begin{array}{l} h02 + h21 + h13 + h22 + h23 + v11 + v31 + v51 + v61 + z21 + z33 + z34 + z43 \\ + z44 + z37 \\ h11 + h03 + h21 + h22 + h14 + h23 + h24 + v12 + v32 + v52 + v62 + z22 + z34 \\ + z35 + z44 + z38 \\ h01 + h11 + h12 + h04 + h22 + h23 + h24 + v13 + v33 + v53 + z31 + v63 + z23 \\ + z41 + z35 + z36 \\ h01 + h12 + h21 + h22 + h24 + v14 + v34 + v54 + z32 + v64 + z24 + z33 + z42 \\ + z34 + z43 + z44 + z36 \\ h02 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + v15 + v35 + v55 \\ + z33 + v65 + z25 + z36 + z46 \\ h03 + h04 + h13 + h22 + h14 + h23 + h34 + v16 + z31 + v36 + v56 + z34 + v66 \\ + z26 + z37 + z47 \\ h21 + h04 + h31 + h14 + h23 + h24 + v17 + z31 + z32 + v37 + v57 + z35 + v67 \\ + z27 + z45 + z38 + z48 \\ h01 + h02 + h11 + h03 + h12 + h21 + h04 + h13 + h14 + h32 + h24 + h33 + h34 \\ + v18 + z32 + v38 + z35 + v58 + z45 + v68 + z28 \end{array} \right\} \\
K_{6_2} = & \left. \begin{array}{l} h01 + h02 + h11 + h03 + h12 + h04 + h14 + h23 + v61 + z32 + z33 + z42 + z43 \\ + z35 + z36 + z38 \\ h02 + h11 + h03 + h12 + h21 + h04 + h13 + h24 + v62 + z31 + z41 + z33 + z34 \\ + z43 + z35 + z44 + z36 + z37 \\ h11 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + v63 + z32 + z42 + z34 + z35 \\ + z44 + z36 + z37 + z38 \\ h01 + h02 + h11 + h03 + h13 + h22 + z31 + z32 + z41 + v64 + z42 + z35 + z37 \\ h02 + h12 + h22 + h23 + h33 + z31 + z33 + v65 + z34 + z36 + z37 + z46 + z47 \\ h03 + h21 + h13 + h31 + h23 + h24 + h34 + z32 + z34 + v66 + z35 + z45 + z37 \\ + z38 + z47 + z48 \\ h01 + h11 + h04 + h22 + h31 + h14 + h32 + h24 + z31 + z33 + v67 + z36 + z46 \\ + z38 + z48 \\ h01 + h11 + h21 + h22 + h32 + z32 + z33 + z35 + z36 + z45 + v68 + z46 \end{array} \right\} \\
K_{6_3} = & \left. \begin{array}{l} h12 + h04 + h13 + h22 + h14 + h23 + h34 + v61 + z42 + z43 + z45 + z46 + z48 \\ h01 + h21 + h13 + h31 + h14 + h23 + h24 + v62 + z41 + z43 + z44 + z45 + z46 \\ + z47 \\ h02 + h22 + h14 + h32 + h24 + v63 + z42 + z44 + z45 + z46 + z47 + z48 \\ h11 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + z41 + v64 + z42 \\ + z45 + z47 \\ h12 + h21 + h22 + h31 + h14 + h34 + z41 + v65 + z43 + z44 + z46 + z47 \\ h11 + h13 + h22 + h31 + h23 + h32 + z42 + v66 + z44 + z45 + z47 + z48 \\ h11 + h12 + h21 + h14 + h23 + h32 + h24 + h33 + z41 + z43 + v67 + z46 + z48 \\ h11 + h21 + h13 + h14 + h24 + h33 + z42 + z43 + z45 + v68 + z46 \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
K_{64} = & \left. \begin{array}{l} h12 + h04 + h13 + h22 + h14 + h23 + h34 + v01 + v21 + v41 + z11 + z42 + z43 \\ + z45 + z46 + z48 \\ h01 + h21 + h13 + h31 + h14 + h23 + h24 + v02 + v22 + v42 + z12 + z41 + z43 \\ + z44 + z45 + z46 + z47 \\ h02 + h22 + h14 + h32 + h24 + v03 + v23 + v43 + z13 + z42 + z44 + z45 + z46 \\ + z47 + z48 \\ h11 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + v04 + v24 + v44 \\ + z14 + z41 + z42 + z45 + z47 \\ h12 + h21 + h22 + h31 + h14 + h34 + v05 + v25 + v45 + z41 + z15 + z43 + z44 \\ + z46 + z47 \\ h11 + h13 + h22 + h31 + h23 + h32 + v06 + v26 + v46 + z42 + z16 + z44 + z45 \\ + z47 + z48 \\ h11 + h12 + h21 + h14 + h23 + h32 + h24 + h33 + v07 + v27 + z41 + v47 + z43 \\ + z17 + z46 + z48 \\ h11 + h21 + h13 + h14 + h24 + h33 + v08 + v28 + z42 + z43 + v48 + z18 + z45 \\ + z46 \end{array} \right\} \\
K_{71} = & \left. \begin{array}{l} h01 + h11 + h03 + h12 + h13 + h23 + h33 + h34 + v01 + v21 + v41 + z11 + v71 \\ + z31 + z32 + z34 + z35 + z45 + z37 + z38 + z47 + z48 \\ h01 + h02 + h11 + h12 + h21 + h04 + h13 + h14 + h24 + h34 + v02 + v22 + v42 \\ + z12 + z31 + v72 + z32 + z33 + z36 + z46 + z38 + z48 \\ h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h14 + v03 + v23 + v43 + z13 \\ + z31 + z32 + v73 + z33 + z34 + z35 + z45 + z37 + z47 \\ h02 + h11 + h12 + h04 + h22 + h14 + h32 + h33 + h34 + v04 + v24 + v44 + z31 \\ + z14 + z33 + v74 + z36 + z37 + z46 + z47 \\ h01 + h11 + h03 + h12 + h21 + h04 + h31 + h33 + h34 + v05 + v25 + z31 + v45 \\ + z32 + z41 + z15 + z42 + z34 + v75 + z35 + z44 + z37 + z38 \\ h02 + h12 + h04 + h13 + h22 + h32 + h34 + v06 + v26 + z31 + z32 + z41 + v46 \\ + z33 + z42 + z16 + z43 + v76 + z36 + z38 \\ h01 + h11 + h03 + h13 + h31 + h14 + h23 + h33 + v07 + z31 + v27 + z32 + z41 \\ + z33 + z42 + v47 + z34 + z43 + z17 + z35 + z44 + v77 + z37 \\ h02 + h11 + h03 + h14 + h32 + h24 + h33 + v08 + z31 + z41 + v28 + z33 + z43 \\ + v48 + z18 + z36 + z37 + v78 \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
K7_2 = & \left. \begin{array}{l} h01 + h21 + h13 + h32 + h33 + v71 + z32 + z37 + z38 + z47 + z48 \\ h02 + h11 + h22 + h31 + h14 + h33 + h34 + v72 + z33 + z38 + z48 \\ h11 + h03 + h12 + h23 + h32 + h34 + z31 + v73 + z34 + z35 + z45 \\ h12 + h04 + h31 + h32 + h24 + z31 + v74 + z36 + z37 + z46 + z38 + z47 + z48 \\ h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h32 + h33 + z33 + z34 + z43 \\ +v75 + z35 + z44 + z36 + z37 \\ h01 + h02 + h11 + h03 + h04 + h13 + h22 + h31 + h14 + h23 + h32 + h33 + h34 \\ +z34 + z35 + z44 + v76 + z36 + z37 + z38 \\ h02 + h03 + h12 + h21 + h04 + h14 + h23 + h32 + h24 + h33 + h34 + z31 + z41 \\ +z36 + v77 + z37 + z38 \\ h01 + h02 + h11 + h12 + h21 + h04 + h31 + h32 + h24 + h34 + z32 + z33 + z42 \\ +z34 + z43 + z35 + z44 + z36 + v78 + z38 \\ h12 + h04 + h13 + h32 + h33 + v71 + z33 + z42 + z34 + z43 + z44 + z36 + z37 \\ +z38 + z47 + z48 \\ h01 + h11 + h13 + h31 + h14 + h33 + h34 + v72 + z34 + z43 + z44 + z37 + z38 + z48 \\ h02 + h12 + h14 + h32 + h34 + z31 + v73 + z44 + z45 + z38 \\ h11 + h03 + h12 + h04 + h31 + h32 + z32 + z41 + z33 + z42 + v74 + z34 + z43 \\ +z35 + z44 + z36 + z37 + z46 + z38 + z47 + z48 \\ h01 + h11 + h12 + h32 + h24 + h34 + z31 + z32 + z34 + z43 + v75 + z44 + z45 \\ +z37 + z46 + z38 + z48 \\ h02 + h12 + h21 + h13 + h31 + h33 + z31 + z32 + z33 + z44 + v76 + z45 + z46 \\ +z38 + z47 \\ h11 + h03 + h13 + h22 + h31 + h14 + h32 + h34 + z31 + z32 + z41 + z33 + z34 \\ +z35 + z45 + v77 + z46 + z47 + z48 \\ h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + z33 + z42 + z43 + z44 \\ +z36 + z45 + z37 + v78 + z38 + z47 \end{array} \right\} \\
K7_3 = & \left. \begin{array}{l} h01 + h11 + h13 + h32 + h33 + v71 + z32 + z37 + z38 + z47 + z48 \\ h02 + h11 + h22 + h31 + h14 + h33 + h34 + v72 + z33 + z38 + z48 \\ h11 + h03 + h12 + h23 + h32 + h34 + z31 + v73 + z34 + z35 + z45 \\ h12 + h04 + h31 + h32 + h24 + h33 + h34 + z31 + z32 + z34 + z43 + z44 + z36 + z37 \\ +z38 + z47 + z48 \\ h01 + h11 + h13 + h31 + h14 + h33 + h34 + v72 + z34 + z43 + z44 + z37 + z38 + z48 \\ h02 + h12 + h14 + h32 + h34 + z31 + v73 + z44 + z45 + z38 \\ h11 + h03 + h12 + h04 + h31 + h32 + z32 + z41 + z33 + z42 + v74 + z34 + z43 \\ +z35 + z44 + z36 + z37 + z46 + z38 + z47 + z48 \\ h01 + h11 + h12 + h32 + h24 + h34 + z31 + z32 + z34 + z43 + v75 + z44 + z45 \\ +z37 + z46 + z38 + z48 \\ h02 + h12 + h21 + h13 + h31 + h33 + z31 + z32 + z33 + z44 + v76 + z45 + z46 \\ +z38 + z47 \\ h11 + h03 + h13 + h22 + h31 + h14 + h32 + h34 + z31 + z32 + z41 + z33 + z34 \\ +z35 + z45 + v77 + z46 + z47 + z48 \\ h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + z33 + z42 + z43 + z44 \\ +z36 + z45 + z37 + v78 + z38 + z47 \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
K_{74} = & \left( \begin{array}{l}
h12 + h04 + h13 + h32 + h33 + v11 + v31 + v51 + v61 + z21 + z33 + z42 + z34 + z43 \\
+ z44 + z36 + z37 + z38 + z47 + z48 \\
h01 + h11 + h13 + h31 + h14 + h33 + h34 + v12 + v32 + v52 + v62 + z22 + z34 + z43 \\
+ z44 + z37 + z38 + z48 \\
h02 + h12 + h14 + h32 + h34 + v13 + v33 + v53 + z31 + v63 + z23 + z44 + z45 + z38 \\
h11 + h03 + h12 + h04 + h31 + h32 + v14 + v34 + v54 + z32 + z41 + v64 + z24 + z33 \\
+ z42 + z34 + z43 + z35 + z44 + z36 + z37 + z46 + z38 + z47 + z48 \\
h01 + h11 + h12 + h32 + h24 + h34 + v15 + v35 + z31 + z32 + v55 + v65 + z25 + z34 \\
+ z43 + z44 + z45 + z37 + z46 + z38 + z48 \\
h02 + h12 + h21 + h13 + h31 + h33 + v16 + z31 + v36 + z32 + z33 + v56 + v66 + z26 \\
+ z44 + z45 + z46 + z38 + z47 \\
h11 + h03 + h13 + h22 + h31 + h14 + h32 + h34 + v17 + z31 + z32 + z41 + v37 + z33 \\
+ z34 + v57 + z35 + v67 + z27 + z45 + z46 + z47 + z48 \\
h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + v18 + z33 + z42 + v38 + z43 \\
+ z44 + v58 + z36 + z45 + v68 + z28 + z37 + z38 + z47 \\
h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + v11 + v31 + v51 + v61 + z21 + v81 \\
+ z32 + z42 + z35 + z37 \\
h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + v12 + v32 + v52 + v62 + z22 \\
+ v82 + z33 + z43 + z35 + z36 + z38 \\
h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + v13 + v33 + v53 + z31 + v63 + z23 \\
+ z41 + v83 + z34 + z35 + z44 + z36 + z37 \\
h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + v14 + v34 + z31 + v54 + z41 \\
+ v64 + z24 + v84 + z36 + z38 \\
h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + v15 + v35 + z31 + v55 + z33 \\
+ v65 + z25 + z35 + v85 + z36 + z45 + z37 + z46 + z47 \\
h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + v16 + z31 + v36 + z32 \\
+ v56 + z34 + v66 + z26 + z35 + z36 + z45 + v86 + z37 + z46 + z38 + z47 + z48 \\
h02 + h03 + h21 + h04 + h13 + h22 + h31 + h32 + h24 + h33 + h34 + v17 + z31 + z32 \\
+ v37 + z33 + v57 + v67 + z27 + z36 + z37 + z46 + v87 + z38 + z47 + z48 \\
h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + v18 + z32 + v38 + z34 + z35 \\
+ v58 + z36 + z45 + v68 + z28 + z46 + z38 + v88 + z48
\end{array} \right)
\end{aligned}$$

$$\begin{aligned}
K_{82} = & \left. \begin{array}{l} h01 + h02 + h11 + h21 + h23 + h33 + z31 + v81 + z41 + z33 + z43 + z35 \\ h02 + h03 + h12 + h21 + h22 + h31 + h24 + h34 + z31 + z32 + z41 + v82 + z42 + z34 \\ +z44 + z36 \\ h01 + h03 + h21 + h04 + h13 + h22 + h31 + h23 + h32 + z31 + z32 + z41 + z33 + z42 \\ +v83 + z43 + z37 \\ h01 + h04 + h22 + h14 + h32 + h24 + z32 + z42 + z34 + v84 + z44 + z38 \\ h11 + h12 + h21 + h04 + h22 + h31 + h23 + h32 + h24 + h33 + h34 + z32 + z33 + z34 \\ +v85 + z38 + z48 \\ h01 + h12 + h13 + h22 + h23 + h32 + h24 + h33 + h34 + z33 + z34 + z35 + z45 + v86 \\ h02 + h11 + h13 + h14 + h23 + h24 + h33 + h34 + z34 + z36 + z46 + v87 \\ h11 + h03 + h21 + h04 + h22 + h31 + h14 + h23 + h32 + h33 + z31 + z32 + z33 + z34 \\ +z37 + z38 + z47 + v88 + z48 \end{array} \right\} \\
K_{83} = & \left. \begin{array}{l} h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + v81 + z41 + z43 + z35 + z36 \\ +z37 + z46 + z47 \\ h01 + h02 + h22 + h31 + h23 + h24 + h33 + z41 + v82 + z42 + z35 + z44 + z36 \\ +z45 + z37 + z38 + z47 + z48 \\ h02 + h03 + h31 + h23 + h32 + h24 + h34 + z41 + z42 + v83 + z43 + z36 + z37 \\ +z46 + z38 + z48 \\ h03 + h21 + h22 + h31 + h23 + h33 + h34 + z42 + v84 + z35 + z44 + z36 + z45 \\ +z46 + z38 \\ h22 + h14 + h24 + h33 + z32 + z34 + z43 + v85 + z48 \\ h11 + h21 + h31 + h23 + h34 + z31 + z41 + z33 + z44 + z45 + v86 \\ h12 + h21 + h22 + h31 + h32 + h24 + z31 + z32 + z41 + z42 + z34 + z46 + v87 \\ h21 + h13 + h14 + h23 + h32 + h24 + z31 + z33 + z42 + z34 + z47 + v88 + z48 \end{array} \right\} \\
K_{84} = & \left. \begin{array}{l} h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + v01 + v21 + v41 + z11 + v71 \\ +z41 + z43 + z35 + z36 + z37 + z46 + z47 \\ h01 + h02 + h22 + h31 + h23 + h24 + h33 + v02 + v22 + v42 + z12 + v72 + z41 \\ +z42 + z35 + z44 + z36 + z45 + z37 + z38 + z47 + z48 \\ h02 + h03 + h31 + h23 + h32 + h24 + h34 + v03 + v23 + v43 + z13 + z41 + v73 \\ +z42 + z43 + z36 + z37 + z46 + z38 + z48 \\ h03 + h21 + h22 + h31 + h23 + h33 + h34 + v04 + v24 + v44 + z14 + z42 + v74 \\ +z35 + z44 + z36 + z45 + z46 + z38 \\ h22 + h14 + h24 + h33 + v05 + v25 + v45 + z32 + z15 + z34 + z43 + v75 + z48 \\ h11 + h21 + h31 + h23 + h34 + v06 + v26 + z31 + z41 + v46 + z33 + z16 + z44 \\ +v76 + z45 \\ h12 + h21 + h22 + h31 + h32 + h24 + v07 + z31 + v27 + z32 + z41 + z42 + v47 \\ +z34 + z17 + v77 + z46 \\ h21 + h13 + h14 + h23 + h32 + h24 + v08 + z31 + v28 + z33 + z42 + z34 + v48 \\ +z18 + v78 + z47 + z48 \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
K_{9_1} = & \left. \begin{array}{l} h02 + h12 + h21 + h31 + h23 + v01 + v21 + v41 + z11 + v71 + z31 + z32 + v91 \\ + z34 + z36 + z37 + z46 + z38 + z47 + z48 \\ h03 + h21 + h13 + h22 + h32 + h24 + v02 + v22 + v42 + z12 + z31 + v72 + z32 \\ + z33 + v92 + z37 + z38 + z47 + z48 \\ h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + v03 + v23 + v43 + z13 + z31 \\ + z32 + v73 + z33 + z34 + v93 + z38 + z48 \\ h01 + h11 + h22 + h24 + h34 + v04 + v24 + v44 + z31 + z14 + z33 + v74 + z35 \\ + v94 + z36 + z45 + z37 + z46 + z38 + z47 + z48 \\ h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + v05 + v25 + z31 + v45 \\ + z41 + z15 + v75 + z35 + v95 + z38 \\ h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + v06 + v26 + z32 + v46 + z42 \\ + z16 + z35 + v76 + z36 + v96 \\ h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + v07 + v27 + z33 + v47 \\ + z43 + z17 + z36 + v77 + z37 + v97 \\ h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + v08 + v28 + z34 + v48 + z44 \\ + z18 + z37 + v78 + v98 \end{array} \right\} \\
K_{9_2} = & \left. \begin{array}{l} h01 + h11 + h03 + h21 + h13 + z32 + v91 + z35 + z36 + z45 + z46 \\ h01 + h02 + h11 + h12 + h04 + h22 + h14 + z33 + v92 + z36 + z37 + z46 + z47 \\ h01 + h02 + h11 + h03 + h12 + h13 + h23 + z31 + z34 + v93 + z35 + z45 + z37 \\ + z38 + z47 + z48 \\ h02 + h12 + h04 + h14 + h24 + z31 + z35 + v94 + z45 + z38 + z48 \\ h01 + h02 + h11 + h03 + h12 + h04 + h13 + h31 + h14 + z31 + z32 + z41 + z42 \\ + z36 + v95 + z38 \\ h02 + h03 + h12 + h04 + h13 + h14 + h32 + z32 + z33 + z42 + z43 + z35 + z37 \\ + v96 \\ h03 + h04 + h13 + h14 + h33 + z31 + z41 + z33 + z34 + z43 + z35 + z44 + z36 \\ + z38 + v97 \\ h01 + h02 + h11 + h03 + h12 + h13 + h34 + z31 + z41 + z34 + z35 + z44 + z37 \\ + z38 + v98 \end{array} \right\}
\end{aligned}$$

【0108】

次に、ステップS103の変数移項処理を実行する。上記K<sub>11</sub>, K<sub>12</sub>, K<sub>13</sub>, K<sub>14</sub>, K<sub>21</sub>, ..., K<sub>91</sub>, K<sub>92</sub>の結果に基づいて、上記の連立線形方程式を変形し、右辺がz×x, v×xの項のみを含むように変形すると、以下のように表せる。

【0109】

【数 3 4】

$$\begin{aligned}k_{111} &= v11 + z21 \\k_{112} &= v12 + z22 \\k_{113} &= v13 + z23 \\k_{114} &= v14 + z24 \\k_{115} &= v15 + z25 \\k_{116} &= v16 + z26 \\k_{117} &= v17 + z27 \\k_{118} &= v18 + z28\end{aligned}$$

$$\begin{aligned}
h_{11} + h_{21} + h_{13} + k_{121} &= v_{11} + z_{32} + z_{42} \\
h_{11} + h_{12} + h_{22} + h_{14} + k_{122} &= v_{12} + z_{33} + z_{43} \\
h_{11} + h_{12} + h_{13} + h_{23} + k_{123} &= v_{13} + z_{31} + z_{41} + z_{34} + z_{44} \\
h_{12} + h_{14} + h_{24} + k_{124} &= v_{14} + z_{31} + z_{41} \\
h_{01} + h_{02} + h_{03} + h_{04} + h_{31} + k_{125} &= v_{15} + z_{36} + z_{46} + z_{38} + z_{48} \\
h_{02} + h_{03} + h_{04} + h_{32} + k_{126} &= v_{16} + z_{35} + z_{45} + z_{37} + z_{47} \\
h_{03} + h_{04} + h_{33} + k_{127} &= v_{17} + z_{35} + z_{36} + z_{45} + z_{46} + z_{38} + z_{48} \\
h_{01} + h_{02} + h_{03} + h_{34} + k_{128} &= v_{18} + z_{35} + z_{45} + z_{37} + z_{38} + z_{47} + z_{48} \\
h_{01} + h_{03} + k_{131} &= v_{11} + z_{42} + z_{35} + z_{36} + z_{45} + z_{46} \\
h_{01} + h_{02} + h_{04} + k_{132} &= v_{12} + z_{43} + z_{36} + z_{37} + z_{46} + z_{47} \\
h_{01} + h_{02} + h_{03} + k_{133} &= v_{13} + z_{41} + z_{35} + z_{44} + z_{45} + z_{37} + z_{38} + z_{47} + z_{48} \\
h_{02} + h_{04} + k_{134} &= v_{14} + z_{41} + z_{35} + z_{45} + z_{38} + z_{48} \\
h_{11} + h_{12} + h_{13} + h_{14} + k_{135} &= v_{15} + z_{31} + z_{32} + z_{41} + z_{42} + z_{46} + z_{48} \\
h_{12} + h_{13} + h_{14} + k_{136} &= v_{16} + z_{32} + z_{33} + z_{42} + z_{43} + z_{45} + z_{47} \\
h_{13} + h_{14} + k_{137} &= v_{17} + z_{31} + z_{41} + z_{33} + z_{34} + z_{43} + z_{44} + z_{45} + z_{46} + z_{48} \\
h_{11} + h_{12} + h_{13} + z_{31} + k_{138} &= v_{18} + z_{41} + z_{34} + z_{44} + z_{45} + z_{47} + z_{48} \\
h_{01} + h_{03} + k_{141} &= v_{01} + z_{11} + z_{42} + z_{35} + z_{36} + z_{45} + z_{46} \\
h_{01} + h_{02} + h_{04} + k_{142} &= v_{02} + z_{12} + z_{43} + z_{36} + z_{37} + z_{46} + z_{47} \\
h_{01} + h_{02} + h_{03} + k_{143} &= v_{03} + z_{13} + z_{41} + z_{35} + z_{44} + z_{45} + z_{37} + z_{38} + \\
&z_{47} + z_{48} \\
h_{02} + h_{04} + k_{144} &= v_{04} + z_{14} + z_{41} + z_{35} + z_{45} + z_{38} + z_{48} \\
h_{11} + h_{12} + h_{13} + h_{14} + k_{145} &= v_{05} + z_{31} + z_{32} + z_{41} + z_{15} + z_{42} + z_{46} + z_{48} \\
h_{12} + h_{13} + h_{14} + k_{146} &= v_{06} + z_{32} + z_{33} + z_{42} + z_{16} + z_{43} + z_{45} + z_{47} \\
h_{13} + h_{14} + k_{147} &= v_{07} + z_{31} + z_{41} + z_{33} + z_{34} + z_{43} + z_{17} + z_{44} + z_{45} + \\
&z_{46} + z_{48} \\
h_{11} + h_{12} + h_{13} + k_{148} &= v_{08} + z_{31} + z_{41} + z_{34} + z_{44} + z_{18} + z_{45} + z_{47} + z_{48} \\
k_{211} &= v_{01} + v_{21} + z_{11} \\
k_{212} &= v_{02} + v_{22} + z_{12} \\
k_{213} &= v_{03} + v_{23} + z_{13} \\
k_{214} &= v_{04} + v_{24} + z_{14} \\
k_{215} &= v_{05} + v_{25} + z_{15} \\
k_{216} &= v_{06} + v_{26} + z_{16} \\
k_{217} &= v_{07} + v_{27} + z_{17} \\
k_{218} &= v_{08} + v_{28} + z_{18} \\
h_{02} + h_{12} + h_{21} + h_{31} + h_{23} + k_{221} &= v_{21} + z_{31} + z_{32} + z_{34} + z_{36} + z_{37} + \\
&z_{46} + z_{38} + z_{47} + z_{48} \\
h_{03} + h_{21} + h_{13} + h_{22} + h_{32} + h_{24} + k_{222} &= v_{22} + z_{31} + z_{32} + z_{33} + z_{37} + \\
&z_{38} + z_{47} + z_{48}
\end{aligned}$$

$$\begin{aligned}
& h_{01} + h_{11} + h_{21} + h_{04} + h_{22} + h_{14} + h_{23} + h_{33} + k_{23} = v_{23} + z_{31} + \\
& z_{32} + z_{33} + z_{34} + z_{38} + z_{48} \\
& h_{01} + h_{11} + h_{22} + h_{24} + h_{34} + k_{24} = v_{24} + z_{31} + z_{33} + z_{35} + z_{36} + z_{45} + \\
& z_{37} + z_{46} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{02} + h_{12} + h_{04} + h_{31} + h_{14} + h_{32} + h_{33} + h_{34} + k_{25} = v_{25} + \\
& z_{31} + z_{41} + z_{35} + z_{38} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{13} + h_{32} + h_{33} + h_{34} + k_{26} = v_{26} + z_{32} + \\
& z_{42} + z_{35} + z_{36} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{12} + h_{04} + h_{14} + h_{33} + h_{34} + k_{27} = v_{27} + \\
& z_{33} + z_{43} + z_{36} + z_{37} \\
& h_{01} + h_{11} + h_{03} + h_{13} + h_{31} + h_{14} + h_{32} + h_{33} + k_{28} = v_{28} + z_{34} + z_{44} + z_{37} \\
& h_{01} + h_{11} + h_{12} + h_{31} + h_{33} + k_{31} = v_{21} + z_{32} + z_{41} + z_{33} + z_{34} + z_{43} + \\
& z_{35} + z_{36} + z_{37} + z_{46} + z_{38} + z_{47} + z_{48} \\
& h_{02} + h_{12} + h_{13} + h_{31} + h_{32} + h_{34} + k_{32} = v_{22} + z_{41} + z_{33} + z_{42} + z_{34} + \\
& z_{44} + z_{36} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{11} + h_{03} + h_{13} + h_{31} + h_{14} + h_{32} + h_{33} + k_{33} = v_{23} + z_{41} + z_{42} + \\
& z_{34} + z_{43} + z_{37} + z_{38} + z_{48} \\
& h_{11} + h_{04} + h_{14} + h_{32} + h_{34} + k_{34} = v_{24} + z_{31} + z_{32} + z_{33} + z_{42} + z_{34} + \\
& z_{35} + z_{44} + z_{36} + z_{45} + z_{37} + z_{46} + z_{47} + z_{48} \\
& h_{01} + h_{02} + h_{11} + h_{21} + h_{22} + h_{14} + h_{23} + h_{24} + k_{35} = v_{25} + z_{31} + \\
& z_{32} + z_{41} + z_{33} + z_{34} + z_{35} + z_{48} \\
& h_{02} + h_{11} + h_{03} + h_{12} + h_{22} + h_{23} + h_{24} + k_{36} = v_{26} + z_{32} + z_{33} + \\
& z_{42} + z_{34} + z_{36} + z_{45} \\
& h_{01} + h_{03} + h_{12} + h_{04} + h_{13} + h_{23} + h_{24} + k_{37} = v_{27} + z_{33} + z_{34} + \\
& z_{43} + z_{37} + z_{46} \\
& h_{01} + h_{21} + h_{04} + h_{13} + h_{22} + h_{23} + z_{31} + z_{32} + k_{38} = v_{28} + z_{33} + z_{44} + \\
& z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{11} + h_{12} + h_{31} + h_{33} + k_{41} = v_{11} + z_{21} + z_{32} + z_{41} + z_{33} + z_{34} + \\
& z_{43} + z_{35} + z_{36} + z_{37} + z_{46} + z_{38} + z_{47} + z_{48} \\
& h_{02} + h_{12} + h_{13} + h_{31} + h_{32} + h_{34} + k_{42} = v_{12} + z_{22} + z_{41} + z_{33} + z_{42} + \\
& z_{34} + z_{44} + z_{36} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{11} + h_{03} + h_{13} + h_{31} + h_{14} + h_{32} + h_{33} + k_{43} = v_{13} + z_{23} + z_{41} + \\
& z_{42} + z_{34} + z_{43} + z_{37} + z_{38} + z_{48} \\
& h_{11} + h_{04} + h_{14} + h_{32} + h_{34} + k_{44} = v_{14} + z_{31} + z_{32} + z_{24} + z_{33} + z_{42} + \\
& z_{34} + z_{35} + z_{44} + z_{36} + z_{45} + z_{37} + z_{46} + z_{47} + z_{48} \\
& h_{01} + h_{02} + h_{11} + h_{21} + h_{22} + h_{14} + h_{23} + h_{24} + k_{45} = v_{15} + z_{31} + \\
& z_{32} + z_{41} + z_{33} + z_{25} + z_{34} + z_{35} + z_{48} \\
& h_{02} + h_{11} + h_{03} + h_{12} + h_{22} + h_{23} + h_{24} + k_{46} = v_{16} + z_{32} + z_{33} + \\
& z_{42} + z_{34} + z_{26} + z_{36} + z_{45}
\end{aligned}$$

$$\begin{aligned}
& h_{01} + h_{03} + h_{12} + h_{04} + h_{13} + h_{23} + h_{24} + k_{247} = v_{17} + z_{33} + z_{34} + \\
& z_{43} + z_{27} + z_{37} + z_{46} \\
& h_{01} + h_{21} + h_{04} + h_{13} + h_{22} + h_{23} + h_{31} + k_{248} = v_{18} + z_{32} + z_{33} + z_{44} + \\
& z_{28} + z_{38} + z_{47} + z_{48} \\
& k_{3_{11}} = v_{11} + v_{31} + z_{21} \\
& k_{3_{12}} = v_{12} + v_{32} + z_{22} \\
& k_{3_{13}} = v_{13} + v_{33} + z_{23} \\
& k_{3_{14}} = v_{14} + v_{34} + z_{24} \\
& k_{3_{15}} = v_{15} + v_{35} + z_{25} \\
& k_{3_{16}} = v_{16} + v_{36} + z_{26} \\
& k_{3_{17}} = v_{17} + v_{37} + z_{27} \\
& k_{3_{18}} = v_{18} + v_{38} + z_{28} \\
& h_{02} + h_{03} + h_{04} + h_{13} + h_{22} + h_{31} + h_{32} + h_{33} + k_{3_{21}} = v_{31} + z_{32} + \\
& z_{42} + z_{35} + z_{37} \\
& h_{11} + h_{03} + h_{04} + h_{31} + h_{14} + h_{23} + h_{32} + h_{33} + h_{34} + k_{3_{22}} = v_{32} + \\
& z_{33} + z_{43} + z_{35} + z_{36} + z_{38} \\
& h_{11} + h_{12} + h_{21} + h_{04} + h_{32} + h_{24} + h_{33} + h_{34} + k_{3_{23}} = v_{33} + z_{31} + \\
& z_{41} + z_{34} + z_{35} + z_{44} + z_{36} + z_{37} \\
& h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{31} + h_{32} + h_{34} + k_{3_{24}} = v_{34} + \\
& z_{31} + z_{41} + z_{36} + z_{38} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{22} + h_{31} + h_{32} + h_{24} + h_{34} + k_{3_{25}} = v_{35} + \\
& z_{31} + z_{33} + z_{35} + z_{36} + z_{45} + z_{37} + z_{46} + z_{47} \\
& h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{31} + h_{23} + h_{32} + h_{33} + z_{31} + k_{3_{26}} = \\
& v_{36} + z_{32} + z_{34} + z_{35} + z_{36} + z_{45} + z_{37} + z_{46} + z_{38} + z_{47} + z_{48} \\
& h_{02} + h_{03} + h_{21} + h_{04} + h_{13} + h_{22} + h_{31} + h_{32} + h_{24} + h_{33} + h_{34} + z_{31} + \\
& z_{32} + k_{3_{27}} = v_{37} + z_{33} + z_{36} + z_{37} + z_{46} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{02} + h_{21} + h_{04} + h_{31} + h_{14} + h_{23} + h_{24} + h_{33} + z_{32} + k_{3_{28}} = \\
& v_{38} + z_{34} + z_{35} + z_{36} + z_{45} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{03} + h_{21} + h_{04} + h_{22} + h_{31} + k_{3_{31}} = v_{31} + z_{42} + z_{35} + \\
& z_{38} + z_{47} + z_{48} \\
& h_{02} + h_{03} + h_{04} + h_{22} + h_{23} + k_{3_{32}} = v_{32} + z_{43} + z_{35} + z_{36} + z_{48} \\
& h_{03} + h_{21} + h_{04} + h_{23} + h_{24} + h_{33} + k_{3_{33}} = v_{33} + z_{41} + z_{44} + z_{36} + z_{45} + z_{37} \\
& h_{01} + h_{02} + h_{03} + h_{21} + h_{24} + h_{34} + k_{3_{34}} = v_{34} + z_{41} + z_{37} + z_{46} + z_{47} + z_{48} \\
& h_{11} + h_{12} + h_{21} + h_{13} + h_{24} + h_{33} + h_{34} + k_{3_{35}} = v_{35} + z_{31} + z_{34} + \\
& z_{43} + z_{44} + z_{45} + z_{46} + z_{47} \\
& h_{11} + h_{12} + h_{21} + h_{13} + h_{22} + h_{14} + h_{34} + z_{31} + k_{3_{36}} = v_{36} + z_{32} + \\
& z_{44} + z_{45} + z_{46} + z_{47} + z_{48} \\
& h_{12} + h_{13} + h_{22} + h_{31} + h_{14} + h_{23} + z_{32} + z_{41} + k_{3_{37}} = v_{37} + z_{33} + z_{46} + \\
& z_{47} + z_{48}
\end{aligned}$$

$$\begin{aligned}
& h_{11} + h_{12} + h_{14} + h_{23} + h_{32} + h_{33} + h_{34} + z_{33} + z_{42} + k_{38} = v_{38} + \\
& z_{43} + z_{44} + z_{45} + z_{46} + z_{48} \\
& h_{01} + h_{02} + h_{03} + h_{21} + h_{04} + h_{22} + h_{31} + k_{41} = v_{01} + v_{21} + z_{11} + \\
& z_{42} + z_{35} + z_{38} + z_{47} + z_{48} \\
& h_{02} + h_{03} + h_{04} + h_{22} + h_{23} + h_{32} + k_{42} = v_{02} + v_{22} + z_{12} + z_{43} + z_{35} + \\
& z_{36} + z_{48} \\
& h_{03} + h_{21} + h_{04} + h_{23} + h_{24} + h_{33} + k_{43} = v_{03} + v_{23} + z_{13} + z_{41} + z_{44} + \\
& z_{36} + z_{45} + z_{37} \\
& h_{01} + h_{02} + h_{03} + h_{21} + h_{24} + h_{34} + k_{44} = v_{04} + v_{24} + z_{14} + z_{41} + z_{37} + \\
& z_{46} + z_{47} + z_{48} \\
& h_{11} + h_{12} + h_{21} + h_{13} + h_{24} + h_{33} + h_{34} + k_{45} = v_{05} + v_{25} + z_{31} + \\
& z_{15} + z_{34} + z_{43} + z_{44} + z_{45} + z_{46} + z_{47} \\
& h_{11} + h_{12} + h_{21} + h_{13} + h_{22} + h_{14} + h_{34} + k_{46} = v_{06} + v_{26} + z_{31} + \\
& z_{32} + z_{16} + z_{44} + z_{45} + z_{46} + z_{47} + z_{48} \\
& h_{12} + h_{13} + h_{22} + h_{31} + h_{14} + h_{23} + k_{47} = v_{07} + v_{27} + z_{32} + z_{41} + z_{33} + \\
& z_{17} + z_{46} + z_{47} + z_{48} \\
& h_{11} + h_{12} + h_{14} + h_{23} + h_{32} + h_{33} + h_{34} + k_{48} = v_{08} + v_{28} + z_{33} + \\
& z_{42} + z_{43} + z_{44} + z_{18} + z_{45} + z_{46} + z_{48} \\
& k_{411} = v_{01} + v_{21} + v_{41} + z_{11} \\
& k_{412} = v_{02} + v_{22} + v_{42} + z_{12} \\
& k_{413} = v_{03} + v_{23} + v_{43} + z_{13} \\
& k_{414} = v_{04} + v_{24} + v_{44} + z_{14} \\
& k_{415} = v_{05} + v_{25} + v_{45} + z_{15} \\
& k_{416} = v_{06} + v_{26} + v_{46} + z_{16} \\
& k_{417} = v_{07} + v_{27} + v_{47} + z_{17} \\
& k_{418} = v_{08} + v_{28} + v_{48} + z_{18} \\
& h_{01} + h_{11} + h_{03} + h_{12} + h_{13} + h_{23} + h_{33} + h_{34} + k_{421} = v_{41} + z_{31} + \\
& z_{32} + z_{34} + z_{35} + z_{45} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{13} + h_{14} + h_{24} + h_{34} + k_{422} = \\
& v_{42} + z_{31} + z_{32} + z_{33} + z_{36} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{13} + h_{22} + h_{31} + h_{14} + k_{423} = v_{43} + \\
& z_{31} + z_{32} + z_{33} + z_{34} + z_{35} + z_{45} + z_{37} + z_{47} \\
& h_{02} + h_{11} + h_{12} + h_{04} + h_{22} + h_{14} + h_{32} + h_{33} + h_{34} + k_{424} = v_{44} + \\
& z_{31} + z_{33} + z_{36} + z_{37} + z_{46} + z_{47} \\
& h_{01} + h_{11} + h_{03} + h_{12} + h_{21} + h_{04} + h_{31} + h_{33} + h_{34} + z_{31} + k_{425} = \\
& v_{45} + z_{32} + z_{41} + z_{42} + z_{34} + z_{35} + z_{44} + z_{37} + z_{38} \\
& h_{02} + h_{12} + h_{04} + h_{13} + h_{22} + h_{32} + h_{34} + z_{31} + z_{32} + z_{41} + k_{426} = \\
& v_{46} + z_{33} + z_{42} + z_{43} + z_{36} + z_{38}
\end{aligned}$$

$$\begin{aligned}
& h_{01} + h_{11} + h_{03} + h_{13} + h_{31} + h_{14} + h_{23} + h_{33} + z_{31} + z_{32} + z_{41} + z_{33} + \\
& z_{42} + k_{427} = v_{47} + z_{34} + z_{43} + z_{35} + z_{44} + z_{37} \\
& h_{02} + h_{11} + h_{03} + h_{14} + h_{32} + h_{24} + h_{33} + z_{31} + z_{41} + z_{33} + z_{43} + k_{428} = \\
& v_{48} + z_{36} + z_{37} \\
& h_{02} + h_{04} + h_{13} + h_{14} + h_{33} + h_{34} + k_{431} = v_{41} + z_{31} + z_{33} + z_{42} + z_{34} + \\
& z_{43} + z_{36} + z_{45} + z_{37} + z_{47} + z_{48} \\
& h_{01} + h_{03} + h_{14} + h_{34} + k_{432} = v_{42} + z_{32} + z_{41} + z_{34} + z_{43} + z_{35} + z_{44} + \\
& z_{37} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{11} + h_{04} + h_{31} + k_{433} = v_{43} + z_{31} + z_{33} + z_{42} + z_{44} + z_{36} + \\
& z_{45} + z_{38} + z_{47} \\
& h_{01} + h_{03} + h_{12} + h_{04} + h_{13} + h_{14} + h_{32} + h_{33} + h_{34} + k_{434} = v_{44} + \\
& z_{32} + z_{41} + z_{33} + z_{42} + z_{35} + z_{36} + z_{46} + z_{47} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{21} + h_{04} + h_{22} + h_{31} + h_{23} + h_{34} + k_{435} = \\
& v_{45} + z_{32} + z_{41} + z_{33} + z_{42} + z_{35} + z_{44} + z_{36} + z_{46} + z_{38} + z_{47} \\
& h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{22} + h_{31} + h_{23} + h_{32} + h_{24} + z_{31} + z_{41} + k_{436} = \\
& v_{46} + z_{33} + z_{42} + z_{34} + z_{43} + z_{35} + z_{36} + z_{45} + z_{37} + z_{47} + z_{48} \\
& h_{03} + h_{04} + h_{13} + h_{22} + h_{23} + h_{32} + h_{24} + h_{33} + z_{32} + z_{41} + z_{42} + k_{437} = \\
& v_{47} + z_{34} + z_{43} + z_{35} + z_{44} + z_{36} + z_{37} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{03} + h_{21} + h_{22} + h_{14} + h_{24} + h_{33} + z_{31} + z_{32} + z_{41} + z_{43} + k_{438} = \\
& v_{48} + z_{35} + z_{45} + z_{37} + z_{46} \\
& h_{02} + h_{04} + h_{13} + h_{14} + h_{33} + h_{34} + k_{441} = v_{11} + v_{31} + z_{21} + z_{31} + z_{33} + \\
& z_{42} + z_{34} + z_{43} + z_{36} + z_{45} + z_{37} + z_{47} + z_{48} \\
& h_{01} + h_{03} + h_{14} + h_{34} + k_{442} = v_{12} + v_{32} + z_{22} + z_{32} + z_{41} + z_{34} + z_{43} + \\
& z_{35} + z_{44} + z_{37} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{11} + h_{04} + h_{31} + k_{443} = v_{13} + v_{33} + z_{31} + z_{23} + z_{33} + z_{42} + \\
& z_{44} + z_{36} + z_{45} + z_{38} + z_{47} \\
& h_{01} + h_{03} + h_{12} + h_{04} + h_{13} + h_{14} + h_{32} + h_{33} + h_{34} + k_{444} = v_{14} + \\
& v_{34} + z_{32} + z_{41} + z_{24} + z_{33} + z_{42} + z_{35} + z_{36} + z_{46} + z_{47} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{21} + h_{04} + h_{22} + h_{31} + h_{23} + h_{34} + k_{445} = \\
& v_{15} + v_{35} + z_{32} + z_{41} + z_{33} + z_{42} + z_{25} + z_{35} + z_{44} + z_{36} + z_{46} + z_{38} + z_{47} \\
& h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{22} + h_{31} + h_{23} + h_{32} + h_{24} + k_{446} = v_{16} + \\
& z_{31} + v_{36} + z_{41} + z_{33} + z_{42} + z_{34} + z_{43} + z_{26} + z_{35} + z_{36} + z_{45} + z_{37} + z_{47} + z_{48} \\
& h_{03} + h_{04} + h_{13} + h_{22} + h_{23} + h_{32} + h_{24} + h_{33} + k_{447} = v_{17} + z_{32} + \\
& z_{41} + v_{37} + z_{42} + z_{34} + z_{43} + z_{35} + z_{44} + z_{27} + z_{36} + z_{37} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{03} + h_{21} + h_{22} + h_{14} + h_{24} + h_{33} + z_{31} + k_{448} = v_{18} + \\
& z_{32} + z_{41} + v_{38} + z_{43} + z_{35} + z_{45} + z_{28} + z_{37} + z_{46} \\
& k_{511} = v_{11} + v_{31} + v_{51} + z_{21} \\
& k_{512} = v_{12} + v_{32} + v_{52} + z_{22} \\
& k_{513} = v_{13} + v_{33} + v_{53} + z_{23}
\end{aligned}$$

$$\begin{aligned}
k_{514} &= v14 + v34 + v54 + z24 \\
k_{515} &= v15 + v35 + v55 + z25 \\
k_{516} &= v16 + v36 + v56 + z26 \\
k_{517} &= v17 + v37 + v57 + z27 \\
k_{518} &= v18 + v38 + v58 + z28 \\
h02 + h21 + h13 + h22 + h23 + k_{521} &= v51 + z33 + z34 + z43 + z44 + z37 \\
h11 + h03 + h21 + h22 + h14 + h23 + h24 + k_{522} &= v52 + z34 + z35 + z44 + z38 \\
h01 + h11 + h12 + h04 + h22 + h23 + h24 + k_{523} &= v53 + z31 + z41 + z35 + z36 \\
h01 + h12 + h21 + h22 + h24 + k_{524} &= v54 + z32 + z33 + z42 + z34 + z43 + \\
&z44 + z36 \\
h02 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + k_{525} &= \\
v55 + z33 + z36 + z46 & \\
h03 + h04 + h13 + h22 + h14 + h23 + h34 + z31 + k_{526} &= v56 + z34 + z37 + z47 \\
h21 + h04 + h31 + h14 + h23 + h24 + z31 + z32 + k_{527} &= v57 + z35 + z45 + \\
z38 + z48 & \\
h01 + h02 + h11 + h03 + h12 + h21 + h04 + h13 + h14 + h32 + h24 + h33 + \\
h34 + z32 + z35 + k_{528} &= v58 + z45 \\
h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + k_{529} &= v51 + z43 + z44 + z47 \\
h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + k_{530} &= v52 + z44 + z45 + z48 \\
h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + k_{531} &= v53 + \\
z41 + z45 + z46 & \\
h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + k_{532} &= \\
v54 + z42 + z43 + z44 + z46 & \\
h11 + h21 + h14 + h34 + k_{533} &= v55 + z43 + z46 \\
h11 + h12 + h22 + h31 + z41 + k_{534} &= v56 + z44 + z47 \\
h12 + h13 + h23 + h32 + z41 + z42 + k_{535} &= v57 + z45 + z48 \\
h13 + h24 + h33 + h34 + z42 + k_{536} &= v58 + z45 \\
h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + k_{537} &= v01 + v21 + \\
v41 + z11 + z43 + z44 + z47 & \\
h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + k_{538} &= v02 + v22 + \\
v42 + z12 + z44 + z45 + z48 & \\
h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + k_{539} &= v03 + \\
v23 + v43 + z13 + z41 + z45 + z46 & \\
h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + k_{540} &= \\
v04 + v24 + v44 + z14 + z42 + z43 + z44 + z46 & \\
h11 + h21 + h14 + h34 + k_{541} &= v05 + v25 + v45 + z15 + z43 + z46 \\
h11 + h12 + h22 + h31 + k_{542} &= v06 + v26 + z41 + v46 + z16 + z44 + z47 \\
h12 + h13 + h23 + h32 + k_{543} &= v07 + v27 + z41 + z42 + v47 + z17 + z45 + z48 \\
h13 + h24 + h33 + h34 + k_{544} &= v08 + v28 + z42 + v48 + z18 + z45
\end{aligned}$$

$$\begin{aligned}
& h_{02} + h_{21} + h_{13} + h_{22} + h_{23} + k_{6_{11}} = v_{11} + v_{31} + v_{51} + v_{61} + z_{21} + z_{33} + \\
& z_{34} + z_{43} + z_{44} + z_{37} \\
& h_{11} + h_{03} + h_{21} + h_{22} + h_{14} + h_{23} + h_{24} + k_{6_{12}} = v_{12} + v_{32} + v_{52} + \\
& v_{62} + z_{22} + z_{34} + z_{35} + z_{44} + z_{38} \\
& h_{01} + h_{11} + h_{12} + h_{04} + h_{22} + h_{23} + h_{24} + k_{6_{13}} = v_{13} + v_{33} + v_{53} + \\
& z_{31} + v_{63} + z_{23} + z_{41} + z_{35} + z_{36} \\
& h_{01} + h_{12} + h_{21} + h_{22} + h_{24} + k_{6_{14}} = v_{14} + v_{34} + v_{54} + z_{32} + v_{64} + z_{24} + \\
& z_{33} + z_{42} + z_{34} + z_{43} + z_{44} + z_{36} \\
& h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{22} + h_{14} + h_{33} + h_{34} + k_{6_{15}} = \\
& v_{15} + v_{35} + v_{55} + z_{33} + v_{65} + z_{25} + z_{36} + z_{46} \\
& h_{03} + h_{04} + h_{13} + h_{22} + h_{14} + h_{23} + h_{34} + k_{6_{16}} = v_{16} + z_{31} + v_{36} + \\
& v_{56} + z_{34} + v_{66} + z_{26} + z_{37} + z_{47} \\
& h_{21} + h_{04} + h_{31} + h_{14} + h_{23} + h_{24} + k_{6_{17}} = v_{17} + z_{31} + z_{32} + v_{37} + v_{57} + \\
& z_{35} + v_{67} + z_{27} + z_{45} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{12} + h_{04} + h_{14} + h_{23} + k_{6_{18}} = v_{18} + z_{32} + v_{38} + z_{35} + v_{58} + z_{45} + v_{68} + z_{28} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{12} + h_{04} + h_{14} + h_{23} + k_{6_{21}} = v_{61} + z_{32} + \\
& z_{33} + z_{42} + z_{43} + z_{35} + z_{36} + z_{38} \\
& h_{02} + h_{11} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{24} + k_{6_{22}} = v_{62} + z_{31} + \\
& z_{41} + z_{33} + z_{34} + z_{43} + z_{35} + z_{44} + z_{36} + z_{37} \\
& h_{11} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{22} + h_{14} + k_{6_{23}} = v_{63} + z_{32} + \\
& z_{42} + z_{34} + z_{35} + z_{44} + z_{36} + z_{37} + z_{38} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{13} + h_{22} + z_{31} + z_{32} + z_{41} + k_{6_{24}} = v_{64} + z_{42} + \\
& z_{35} + z_{37} \\
& h_{02} + h_{12} + h_{22} + h_{23} + h_{33} + z_{31} + z_{33} + k_{6_{25}} = v_{65} + z_{34} + z_{36} + z_{37} + \\
& z_{46} + z_{47} \\
& h_{03} + h_{21} + h_{13} + h_{31} + h_{23} + h_{24} + h_{34} + z_{32} + z_{34} + k_{6_{26}} = v_{66} + \\
& z_{35} + z_{45} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{11} + h_{04} + h_{22} + h_{31} + h_{14} + h_{32} + h_{24} + z_{31} + z_{33} + k_{6_{27}} = \\
& v_{67} + z_{36} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{11} + h_{21} + h_{22} + h_{32} + z_{32} + z_{33} + z_{35} + z_{36} + z_{45} + k_{6_{28}} = v_{68} + z_{46} \\
& h_{12} + h_{04} + h_{13} + h_{22} + h_{14} + h_{23} + h_{34} + k_{6_{31}} = v_{61} + z_{42} + z_{43} + \\
& z_{45} + z_{46} + z_{48} \\
& h_{01} + h_{21} + h_{13} + h_{31} + h_{14} + h_{23} + h_{24} + k_{6_{32}} = v_{62} + z_{41} + z_{43} + \\
& z_{44} + z_{45} + z_{46} + z_{47} \\
& h_{02} + h_{22} + h_{14} + h_{32} + h_{24} + k_{6_{33}} = v_{63} + z_{42} + z_{44} + z_{45} + z_{46} + z_{47} + z_{48} \\
& h_{11} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{22} + h_{14} + h_{33} + h_{34} + z_{41} + k_{6_{34}} = \\
& v_{64} + z_{42} + z_{45} + z_{47} \\
& h_{12} + h_{21} + h_{22} + h_{31} + h_{14} + h_{34} + z_{41} + k_{6_{35}} = v_{65} + z_{43} + z_{44} + z_{46} + z_{47}
\end{aligned}$$

$$\begin{aligned}
& h_{11} + h_{13} + h_{22} + h_{31} + h_{23} + h_{32} + z_{42} + k_{6_{36}} = v_{66} + z_{44} + z_{45} + z_{47} + z_{48} \\
& h_{11} + h_{12} + h_{21} + h_{14} + h_{23} + h_{32} + h_{24} + h_{33} + z_{41} + z_{43} + k_{6_{37}} = \\
& v_{67} + z_{46} + z_{48} \\
& h_{11} + h_{21} + h_{13} + h_{14} + h_{24} + h_{33} + z_{42} + z_{43} + z_{45} + k_{6_{38}} = v_{68} + z_{46} \\
& h_{12} + h_{04} + h_{13} + h_{22} + h_{14} + h_{23} + h_{34} + k_{6_{41}} = v_{01} + v_{21} + v_{41} + \\
& z_{11} + z_{42} + z_{43} + z_{45} + z_{46} + z_{48} \\
& h_{01} + h_{21} + h_{13} + h_{31} + h_{14} + h_{23} + h_{24} + k_{6_{42}} = v_{02} + v_{22} + v_{42} + \\
& z_{12} + z_{41} + z_{43} + z_{44} + z_{45} + z_{46} + z_{47} \\
& h_{02} + h_{22} + h_{14} + h_{32} + h_{24} + k_{6_{43}} = v_{03} + v_{23} + v_{43} + z_{13} + z_{42} + z_{44} + \\
& z_{45} + z_{46} + z_{47} + z_{48} \\
& h_{11} + h_{03} + h_{12} + h_{21} + h_{04} + h_{13} + h_{22} + h_{14} + h_{33} + h_{34} + k_{6_{44}} = \\
& v_{04} + v_{24} + v_{44} + z_{14} + z_{41} + z_{42} + z_{45} + z_{47} \\
& h_{12} + h_{21} + h_{22} + h_{31} + h_{14} + h_{34} + k_{6_{45}} = v_{05} + v_{25} + v_{45} + z_{41} + z_{15} + \\
& z_{43} + z_{44} + z_{46} + z_{47} \\
& h_{11} + h_{13} + h_{22} + h_{31} + h_{23} + h_{32} + k_{6_{46}} = v_{06} + v_{26} + v_{46} + z_{42} + z_{16} + \\
& z_{44} + z_{45} + z_{47} + z_{48} \\
& h_{11} + h_{12} + h_{21} + h_{14} + h_{23} + h_{32} + h_{24} + h_{33} + k_{6_{47}} = v_{07} + v_{27} + \\
& z_{41} + v_{47} + z_{43} + z_{17} + z_{46} + z_{48} \\
& h_{11} + h_{21} + h_{13} + h_{14} + h_{24} + h_{33} + k_{6_{48}} = v_{08} + v_{28} + z_{42} + z_{43} + v_{48} + \\
& z_{18} + z_{45} + z_{46} \\
& h_{01} + h_{11} + h_{03} + h_{12} + h_{13} + h_{23} + h_{33} + h_{34} + k_{7_{11}} = v_{01} + v_{21} + \\
& v_{41} + z_{11} + v_{71} + z_{31} + z_{32} + z_{34} + z_{35} + z_{45} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{13} + h_{14} + h_{24} + h_{34} + k_{7_{12}} = \\
& v_{02} + v_{22} + v_{42} + z_{12} + z_{31} + v_{72} + z_{32} + z_{33} + z_{36} + z_{46} + z_{38} + z_{48} \\
& h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{13} + h_{22} + h_{31} + h_{14} + k_{7_{13}} = v_{03} + \\
& v_{23} + v_{43} + z_{13} + z_{31} + z_{32} + v_{73} + z_{33} + z_{34} + z_{35} + z_{45} + z_{37} + z_{47} \\
& h_{02} + h_{11} + h_{12} + h_{04} + h_{22} + h_{14} + h_{32} + h_{33} + h_{34} + k_{7_{14}} = v_{04} + \\
& v_{24} + v_{44} + z_{31} + z_{14} + z_{33} + v_{74} + z_{36} + z_{37} + z_{46} + z_{47} \\
& h_{01} + h_{11} + h_{03} + h_{12} + h_{21} + h_{04} + h_{31} + h_{33} + h_{34} + k_{7_{15}} = v_{05} + \\
& v_{25} + z_{31} + v_{45} + z_{32} + z_{41} + z_{15} + z_{42} + z_{34} + v_{75} + z_{35} + z_{44} + z_{37} + z_{38} \\
& h_{02} + h_{12} + h_{04} + h_{13} + h_{22} + h_{32} + h_{34} + k_{7_{16}} = v_{06} + v_{26} + z_{31} + \\
& z_{32} + z_{41} + v_{46} + z_{33} + z_{42} + z_{16} + z_{43} + v_{76} + z_{36} + z_{38} \\
& h_{01} + h_{11} + h_{03} + h_{13} + h_{31} + h_{14} + h_{23} + h_{33} + k_{7_{17}} = v_{07} + z_{31} + \\
& v_{27} + z_{32} + z_{41} + z_{33} + z_{42} + v_{47} + z_{34} + z_{43} + z_{17} + z_{35} + z_{44} + v_{77} + z_{37} \\
& h_{02} + h_{11} + h_{03} + h_{14} + h_{32} + h_{24} + h_{33} + k_{7_{18}} = v_{08} + z_{31} + z_{41} + \\
& v_{28} + z_{33} + z_{43} + v_{48} + z_{18} + z_{36} + z_{37} + v_{78} \\
& h_{01} + h_{21} + h_{13} + h_{32} + h_{33} + k_{7_{21}} = v_{71} + z_{32} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{02} + h_{11} + h_{22} + h_{31} + h_{14} + h_{33} + h_{34} + k_{7_{22}} = v_{72} + z_{33} + z_{38} + z_{48} \\
& h_{11} + h_{03} + h_{12} + h_{23} + h_{32} + h_{34} + z_{31} + k_{7_{23}} = v_{73} + z_{34} + z_{35} + z_{45}
\end{aligned}$$

$$\begin{aligned}
& h_{12} + h_{04} + h_{31} + h_{32} + h_{24} + z_{31} + k_{724} = v_{74} + z_{36} + z_{37} + z_{46} + z_{38} + \\
& z_{47} + z_{48} \\
& h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{13} + h_{22} + h_{31} + h_{32} + h_{33} + z_{33} + z_{34} + \\
& z_{43} + k_{725} = v_{75} + z_{35} + z_{44} + z_{36} + z_{37} \\
& h_{01} + h_{02} + h_{11} + h_{03} + h_{04} + h_{13} + h_{22} + h_{31} + h_{14} + h_{23} + h_{32} + h_{33} + \\
& h_{34} + z_{34} + z_{35} + z_{44} + k_{726} = v_{76} + z_{36} + z_{37} + z_{38} \\
& h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{14} + h_{23} + h_{32} + h_{24} + h_{33} + h_{34} + z_{31} + \\
& z_{41} + z_{36} + k_{727} = v_{77} + z_{37} + z_{38} \\
& h_{01} + h_{02} + h_{11} + h_{12} + h_{21} + h_{04} + h_{31} + h_{32} + h_{24} + h_{34} + z_{32} + z_{33} + \\
& z_{42} + z_{34} + z_{43} + z_{35} + z_{44} + z_{36} + k_{728} = v_{78} + z_{38} \\
& h_{12} + h_{04} + h_{13} + h_{32} + h_{33} + k_{731} = v_{71} + z_{33} + z_{42} + z_{34} + z_{43} + z_{44} + \\
& z_{36} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{11} + h_{13} + h_{31} + h_{14} + h_{33} + h_{34} + k_{732} = v_{72} + z_{34} + z_{43} + \\
& z_{44} + z_{37} + z_{38} + z_{48} \\
& h_{02} + h_{12} + h_{14} + h_{32} + h_{34} + z_{31} + k_{733} = v_{73} + z_{44} + z_{45} + z_{38} \\
& h_{11} + h_{03} + h_{12} + h_{04} + h_{31} + h_{32} + z_{32} + z_{41} + z_{33} + z_{42} + k_{734} = \\
& v_{74} + z_{34} + z_{43} + z_{35} + z_{44} + z_{36} + z_{37} + z_{46} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{11} + h_{12} + h_{32} + h_{24} + h_{34} + z_{31} + z_{32} + z_{34} + z_{43} + k_{735} = \\
& v_{75} + z_{44} + z_{45} + z_{37} + z_{46} + z_{38} + z_{48} \\
& h_{02} + h_{12} + h_{21} + h_{13} + h_{31} + h_{33} + z_{31} + z_{32} + z_{33} + z_{44} + k_{736} = \\
& v_{76} + z_{45} + z_{46} + z_{38} + z_{47} \\
& h_{11} + h_{03} + h_{13} + h_{22} + h_{31} + h_{14} + h_{32} + h_{34} + z_{31} + z_{32} + z_{41} + z_{33} + \\
& z_{34} + z_{35} + z_{45} + k_{737} = v_{77} + z_{46} + z_{47} + z_{48} \\
& h_{11} + h_{04} + h_{31} + h_{14} + h_{23} + h_{24} + h_{33} + h_{34} + z_{31} + z_{33} + z_{42} + z_{43} + \\
& z_{44} + z_{36} + z_{45} + z_{37} + k_{738} = v_{78} + z_{38} + z_{47} \\
& h_{12} + h_{04} + h_{13} + h_{32} + h_{33} + k_{741} = v_{11} + v_{31} + v_{51} + v_{61} + z_{21} + z_{33} + \\
& z_{42} + z_{34} + z_{43} + z_{44} + z_{36} + z_{37} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{11} + h_{13} + h_{31} + h_{14} + h_{33} + h_{34} + k_{742} = v_{12} + v_{32} + v_{52} + \\
& v_{62} + z_{22} + z_{34} + z_{43} + z_{44} + z_{37} + z_{38} + z_{48} \\
& h_{02} + h_{12} + h_{14} + h_{32} + h_{34} + k_{743} = v_{13} + v_{33} + v_{53} + z_{31} + v_{63} + z_{23} + \\
& z_{44} + z_{45} + z_{38} \\
& h_{11} + h_{03} + h_{12} + h_{04} + h_{31} + h_{32} + k_{744} = v_{14} + v_{34} + v_{54} + z_{32} + z_{41} + \\
& v_{64} + z_{24} + z_{33} + z_{42} + z_{34} + z_{43} + z_{35} + z_{44} + z_{36} + z_{37} + z_{46} + z_{38} + z_{47} + z_{48} \\
& h_{01} + h_{11} + h_{12} + h_{32} + h_{24} + h_{34} + k_{745} = v_{15} + v_{35} + z_{31} + z_{32} + v_{55} + \\
& v_{65} + z_{25} + z_{34} + z_{43} + z_{44} + z_{45} + z_{37} + z_{46} + z_{38} + z_{48} \\
& h_{02} + h_{12} + h_{21} + h_{13} + h_{31} + h_{33} + k_{746} = v_{16} + z_{31} + v_{36} + z_{32} + z_{33} + \\
& v_{56} + v_{66} + z_{26} + z_{44} + z_{45} + z_{46} + z_{38} + z_{47} \\
& h_{11} + h_{03} + h_{13} + h_{22} + h_{31} + h_{14} + h_{32} + h_{34} + k_{747} = v_{17} + z_{31} + \\
& z_{32} + z_{41} + v_{37} + z_{33} + z_{34} + v_{57} + z_{35} + v_{67} + z_{27} + z_{45} + z_{46} + z_{47} + z_{48}
\end{aligned}$$



$h_{11} + h_{04} + h_{31} + h_{14} + h_{23} + h_{24} + h_{33} + h_{34} + z_{31} + k_{748} = v_{18} +$   
 $z_{33} + z_{42} + v_{38} + z_{43} + z_{44} + v_{58} + z_{36} + z_{45} + v_{68} + z_{28} + z_{37} + z_{38} + z_{47}$   
 $h_{02} + h_{03} + h_{04} + h_{13} + h_{22} + h_{31} + h_{32} + h_{33} + k_{8_{11}} = v_{11} + v_{31} +$   
 $v_{51} + v_{61} + z_{21} + v_{81} + z_{32} + z_{42} + z_{35} + z_{37}$   
 $h_{11} + h_{03} + h_{04} + h_{31} + h_{14} + h_{23} + h_{32} + h_{33} + h_{34} + k_{8_{12}} = v_{12} +$   
 $v_{32} + v_{52} + v_{62} + z_{22} + v_{82} + z_{33} + z_{43} + z_{35} + z_{36} + z_{38}$   
 $h_{11} + h_{12} + h_{21} + h_{04} + h_{32} + h_{24} + h_{33} + h_{34} + k_{8_{13}} = v_{13} + v_{33} +$   
 $v_{53} + z_{31} + v_{63} + z_{23} + z_{41} + v_{83} + z_{34} + z_{35} + z_{44} + z_{36} + z_{37}$   
 $h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{31} + h_{32} + h_{34} + k_{8_{14}} = v_{14} +$   
 $v_{34} + z_{31} + v_{54} + z_{41} + v_{64} + z_{24} + v_{84} + z_{36} + z_{38}$   
 $h_{01} + h_{02} + h_{11} + h_{03} + h_{22} + h_{31} + h_{32} + h_{24} + h_{34} + k_{8_{15}} = v_{15} +$   
 $v_{35} + z_{31} + v_{55} + z_{33} + v_{65} + z_{25} + z_{35} + v_{85} + z_{36} + z_{45} + z_{37} + z_{46} + z_{47}$   
 $h_{01} + h_{02} + h_{03} + h_{12} + h_{21} + h_{04} + h_{31} + h_{23} + h_{32} + h_{33} + k_{8_{16}} =$   
 $v_{16} + z_{31} + v_{36} + z_{32} + v_{56} + z_{34} + v_{66} + z_{26} + z_{35} + z_{36} + z_{45} + v_{86} +$   
 $z_{37} + z_{46} + z_{38} + z_{47} + z_{48}$   
 $h_{02} + h_{03} + h_{21} + h_{04} + h_{13} + h_{22} + h_{31} + h_{32} + h_{24} + h_{33} + h_{34} + k_{8_{17}} = v_{17} +$   
 $z_{31} + z_{32} + v_{37} + z_{33} + v_{57} + v_{67} + z_{27} + z_{36} + z_{37} + z_{46} + v_{87} + z_{38} + z_{47} + z_{48}$   
 $h_{01} + h_{02} + h_{21} + h_{04} + h_{31} + h_{14} + h_{23} + h_{24} + h_{33} + h_{34} + k_{8_{18}} = v_{18} +$   
 $v_{32} + v_{38} + z_{34} + z_{35} + v_{58} + z_{36} + z_{45} + v_{68} + z_{28} + z_{46} + z_{38} + v_{88} + z_{48}$   
 $h_{01} + h_{02} + h_{11} + h_{21} + h_{23} + h_{33} + z_{31} + k_{8_{21}} = v_{81} + z_{41} + z_{33} + z_{43} + z_{35}$   
 $h_{02} + h_{03} + h_{12} + h_{21} + h_{22} + h_{31} + h_{24} + h_{34} + z_{31} + z_{32} + z_{41} + k_{8_{22}} =$   
 $v_{82} + z_{42} + z_{34} + z_{44} + z_{36}$   
 $h_{01} + h_{03} + h_{21} + h_{04} + h_{13} + h_{22} + h_{31} + h_{23} + h_{32} + z_{31} + z_{32} + z_{41} +$   
 $z_{33} + z_{42} + k_{8_{23}} = v_{83} + z_{43} + z_{37}$   
 $h_{01} + h_{04} + h_{22} + h_{14} + h_{32} + h_{24} + z_{32} + z_{42} + z_{34} + k_{8_{24}} = v_{84} + z_{44} + z_{38}$   
 $h_{11} + h_{12} + h_{21} + h_{04} + h_{22} + h_{31} + h_{23} + h_{32} + h_{24} + h_{33} + h_{34} + z_{32} +$   
 $z_{33} + z_{34} + k_{8_{25}} = v_{85} + z_{38} + z_{48}$   
 $h_{01} + h_{12} + h_{13} + h_{22} + h_{23} + h_{32} + h_{24} + h_{33} + h_{34} + z_{33} + z_{34} + z_{35} +$   
 $z_{45} + k_{8_{26}} = v_{86}$   
 $h_{02} + h_{11} + h_{13} + h_{14} + h_{23} + h_{24} + h_{33} + h_{34} + z_{34} + z_{36} + z_{46} + k_{8_{27}} = v_{87}$   
 $h_{11} + h_{03} + h_{21} + h_{04} + h_{22} + h_{31} + h_{14} + h_{23} + h_{32} + h_{33} + z_{31} + z_{32} +$   
 $z_{33} + z_{34} + z_{37} + z_{38} + z_{47} + k_{8_{28}} = v_{88} + z_{48}$   
 $h_{01} + h_{21} + h_{04} + h_{22} + h_{23} + h_{32} + h_{24} + h_{34} + k_{8_{31}} = v_{81} + z_{41} +$   
 $z_{43} + z_{35} + z_{36} + z_{37} + z_{46} + z_{47}$   
 $h_{01} + h_{02} + h_{22} + h_{31} + h_{23} + h_{24} + h_{33} + z_{41} + k_{8_{32}} = v_{82} + z_{42} +$   
 $z_{35} + z_{44} + z_{36} + z_{45} + z_{37} + z_{38} + z_{47} + z_{48}$   
 $h_{02} + h_{03} + h_{31} + h_{23} + h_{32} + h_{24} + h_{34} + z_{41} + z_{42} + k_{8_{33}} = v_{83} +$   
 $z_{43} + z_{36} + z_{37} + z_{46} + z_{38} + z_{48}$   
 $h_{03} + h_{21} + h_{22} + h_{31} + h_{23} + h_{33} + h_{34} + z_{42} + k_{8_{34}} = v_{84} + z_{35} +$

$z44 + z36 + z45 + z46 + z38$   
 $h22 + h14 + h24 + h33 + z32 + z34 + z43 + k8_{35} = v85 + z48$   
 $h11 + h21 + h31 + h23 + h34 + z31 + z41 + z33 + z44 + z45 + k8_{36} = v86$   
 $h12 + h21 + h22 + h31 + h32 + h24 + z31 + z32 + z41 + z42 + z34 + z46 + k8_{37} =$   
 $v87$   
 $h21 + h13 + h14 + h23 + h32 + h24 + z31 + z33 + z42 + z34 + z47 + k8_{38} =$   
 $v88 + z48$   
 $h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + k8_{41} = v01 + v21 +$   
 $v41 + z11 + v71 + z41 + z43 + z35 + z36 + z37 + z46 + z47$   
 $h01 + h02 + h22 + h31 + h23 + h24 + h33 + k8_{42} = v02 + v22 + v42 +$   
 $z12 + v72 + z41 + z42 + z35 + z44 + z36 + z45 + z37 + z38 + z47 + z48$   
 $h02 + h03 + h31 + h23 + h32 + h24 + h34 + k8_{43} = v03 + v23 + v43 +$   
 $z13 + z41 + v73 + z42 + z43 + z36 + z37 + z46 + z38 + z48$   
 $h03 + h21 + h22 + h31 + h23 + h33 + h34 + k8_{44} = v04 + v24 + v44 +$   
 $z14 + z42 + v74 + z35 + z44 + z36 + z45 + z46 + z38$   
 $h22 + h14 + h24 + h33 + k8_{45} = v05 + v25 + v45 + z32 + z15 + z34 + z43 +$   
 $v75 + z48$   
 $h11 + h21 + h31 + h23 + h34 + k8_{46} = v06 + v26 + z31 + z41 + v46 + z33 +$   
 $z16 + z44 + v76 + z45$   
 $h12 + h21 + h22 + h31 + h32 + h24 + k8_{47} = v07 + z31 + v27 + z32 + z41 +$   
 $z42 + v47 + z34 + z17 + v77 + z46$   
 $h21 + h13 + h14 + h23 + h32 + h24 + k8_{48} = v08 + z31 + v28 + z33 + z42 +$   
 $z34 + v48 + z18 + v78 + z47 + z48$   
 $h02 + h12 + h21 + h31 + h23 + k9_{11} = v01 + v21 + v41 + z11 + v71 + z31 +$   
 $z32 + v91 + z34 + z36 + z37 + z46 + z38 + z47 + z48$   
 $h03 + h21 + h13 + h22 + h32 + h24 + k9_{12} = v02 + v22 + v42 + z12 + z31 +$   
 $v72 + z32 + z33 + v92 + z37 + z38 + z47 + z48$   
 $h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + k9_{13} = v03 + v23 +$   
 $v43 + z13 + z31 + z32 + v73 + z33 + z34 + v93 + z38 + z48$   
 $h01 + h11 + h22 + h24 + h34 + k9_{14} = v04 + v24 + v44 + z31 + z14 + z33 +$   
 $v74 + z35 + v94 + z36 + z45 + z37 + z46 + z38 + z47 + z48$   
 $h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + k9_{15} = v05 +$   
 $v25 + z31 + v45 + z41 + z15 + v75 + z35 + v95 + z38$   
 $h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + k9_{16} = v06 + v26 +$   
 $z32 + v46 + z42 + z16 + z35 + v76 + z36 + v96$   
 $h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + k9_{17} = v07 +$   
 $v27 + z33 + v47 + z43 + z17 + z36 + v77 + z37 + v97$   
 $h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + k9_{18} = v08 + v28 +$   
 $z34 + v48 + z44 + z18 + z37 + v78 + v98$

$$\begin{aligned}
 h01 + h11 + h03 + h21 + h13 + z32 + k9_{21} &= v91 + z35 + z36 + z45 + z46 \\
 h01 + h02 + h11 + h12 + h04 + h22 + h14 + z33 + k9_{22} &= v92 + z36 + \\
 z37 + z46 + z47 \\
 h01 + h02 + h11 + h03 + h12 + h13 + h23 + z31 + z34 + k9_{23} &= v93 + \\
 z35 + z45 + z37 + z38 + z47 + z48 \\
 h02 + h12 + h04 + h14 + h24 + z31 + z35 + k9_{24} &= v94 + z45 + z38 + z48 \\
 h01 + h02 + h11 + h03 + h12 + h04 + h13 + h31 + h14 + z31 + z32 + z41 + \\
 z42 + z36 + k9_{25} &= v95 + z38 \\
 h02 + h03 + h12 + h04 + h13 + h14 + h32 + z32 + z33 + z42 + z43 + z35 + \\
 z37 + k9_{26} &= v96 \\
 h03 + h04 + h13 + h14 + h33 + z31 + z41 + z33 + z34 + z43 + z35 + z44 + \\
 z36 + z38 + k9_{27} &= v97 \\
 h01 + h02 + h11 + h03 + h12 + h13 + h34 + z31 + z41 + z34 + z35 + z44 + \\
 z37 + z38 + k9_{28} &= v98
 \end{aligned}$$

## 【0 1 1 0】

次に、ステップS104の行列方程式変換処理を実行する。ここで、ベクトルK, H, U, Vを下記のように設定する。

## 【0 1 1 1】

## 【数35】

$$\begin{aligned}
 K &= (k1_{11}, k1_{12}, \dots, k9_{28}) \\
 H &= (h0_1, h0_2, \dots, h4_4) \\
 U &= (z1_1, z1_2, \dots, z4_4) \\
 V &= (v0_1, v0_2, \dots, v7_4)
 \end{aligned}$$

## 【0 1 1 2】

上記式のように、ベクトルK, H, U, Vを設定すると、上記連立線形方程式は以下のように行列方程式に変換できる。

## 【0 1 1 3】

## 【数36】

$$M_{KH} \begin{pmatrix} {}^t\!K \\ {}^t\!H \end{pmatrix} = M_{UV} \begin{pmatrix} {}^t\!U \\ {}^t\!V \end{pmatrix}$$

## 【0 1 1 4】

なお、上記式において、 $M_{KH}$ ,  $M_{UV}$ は、上記連立線形方程式の係数から成るGF(2)上の行列である。

【0115】

次に、ステップS105のユニタリ変換処理を実行する。

【0116】

【数37】

$$\text{rank } (M_{UV}) = N_r$$

【0117】

とする。また、行列 $M_{UV}$ の行数を $N_m$ とする。上記行列方程式の両辺に左から行変形ユニタリー行列 $Q$ を乗ずることによって、行列 $M_{UV}$ を階段行列に変形することができる。このとき、 $QM_{UV}$ のうち、下 $N_m - N_r$ 行から成る小行列は零行列になる。

【0118】

次に、ステップS106の小行列選択処理を実行する。 $QM_{KH}$ の下 $N_m - N_r$ 行の小行列を $M_{KH}^*$ とおくと、 $M_{KH}^*$ は零行列(○)であり、下記式によって示される。

【0119】

【数38】

$$M_{KH}^* = \text{O}$$

【0120】

次にステップS107の線形関係式生成処理を実行する。この行列方程式を行毎の線形関係式に変換し、 $h01, h02, \dots, h44$ の具体的な値を代入すると、以下のような関係式が得られる。

【0121】

【数39】

$$0x07 = k1_{11} + k1_{21} + k1_{24} + k1_{26} + k1_{31} + k1_{34} + k1_{36} + k1_{42} + k2_{12} + \\ k2_{22} + k3_{11} + k3_{21}$$

$0x66 = k_{112} + k_{121} + k_{122} + k_{127} + k_{131} + k_{132} + k_{137} + k_{143} + k_{213} + k_{223} + k_{312} + k_{322}$   
 $0x9e = k_{113} + k_{122} + k_{123} + k_{125} + k_{128} + k_{132} + k_{133} + k_{135} + k_{138} + k_{141} + k_{144} + k_{211} + k_{214} + k_{221} + k_{224} + k_{313} + k_{323}$   
 $0xdf = k_{114} + k_{123} + k_{125} + k_{133} + k_{135} + k_{141} + k_{211} + k_{221} + k_{314} + k_{324}$   
 $0xe9 = k_{115} + k_{122} + k_{124} + k_{125} + k_{126} + k_{132} + k_{134} + k_{135} + k_{136} + k_{146} + k_{148} + k_{216} + k_{218} + k_{226} + k_{228} + k_{315} + k_{325}$   
 $0x23 = k_{116} + k_{121} + k_{123} + k_{126} + k_{127} + k_{131} + k_{133} + k_{136} + k_{137} + k_{145} + k_{147} + k_{215} + k_{217} + k_{225} + k_{227} + k_{316} + k_{326}$   
 $0x60 = k_{117} + k_{121} + k_{122} + k_{124} + k_{125} + k_{127} + k_{128} + k_{131} + k_{132} + k_{134} + k_{135} + k_{137} + k_{138} + k_{145} + k_{146} + k_{148} + k_{215} + k_{216} + k_{218} + k_{225} + k_{226} + k_{228} + k_{317} + k_{327}$   
 $0xcl = k_{118} + k_{121} + k_{123} + k_{124} + k_{125} + k_{128} + k_{131} + k_{133} + k_{134} + k_{135} + k_{138} + k_{145} + k_{147} + k_{148} + k_{215} + k_{217} + k_{218} + k_{225} + k_{227} + k_{228} + k_{318} + k_{328}$   
 $0x3d = k_{121} + k_{124} + k_{127} + k_{128} + k_{131} + k_{134} + k_{137} + k_{138} + k_{141} + k_{142} + k_{143} + k_{148} + k_{211} + k_{212} + k_{218} + k_{221} + k_{222} + k_{223} + k_{228} + k_{413} + k_{433}$   
 $0x90 = k_{122} + k_{125} + k_{126} + k_{127} + k_{128} + k_{132} + k_{135} + k_{136} + k_{137} + k_{138} + k_{141} + k_{143} + k_{146} + k_{147} + k_{148} + k_{213} + k_{216} + k_{217} + k_{218} + k_{221} + k_{223} + k_{226} + k_{227} + k_{228} + k_{411} + k_{431}$   
 $0xc1 = k_{123} + k_{126} + k_{127} + k_{128} + k_{133} + k_{136} + k_{137} + k_{138} + k_{141} + k_{142} + k_{144} + k_{147} + k_{148} + k_{211} + k_{214} + k_{217} + k_{218} + k_{221} + k_{222} + k_{224} + k_{227} + k_{228} + k_{412} + k_{432}$   
 $0x80 = k_{124} + k_{125} + k_{126} + k_{128} + k_{134} + k_{135} + k_{136} + k_{138} + k_{141} + k_{143} + k_{144} + k_{145} + k_{146} + k_{147} + k_{211} + k_{215} + k_{216} + k_{217} + k_{221} + k_{223} + k_{224} + k_{225} + k_{226} + k_{227} + k_{413} + k_{414} + k_{433} + k_{434}$   
 $0x39 = k_{125} + k_{135} + k_{141} + k_{144} + k_{145} + k_{147} + k_{148} + k_{211} + k_{212} + k_{214} + k_{215} + k_{216} + k_{217} + k_{218} + k_{221} + k_{224} + k_{225} + k_{227} + k_{228} + k_{412} + k_{416} + k_{432} + k_{436}$   
 $0xd2 = k_{126} + k_{136} + k_{141} + k_{142} + k_{146} + k_{148} + k_{211} + k_{212} + k_{213} + k_{216} + k_{217} + k_{218} + k_{221} + k_{222} + k_{226} + k_{228} + k_{413} + k_{417} + k_{433} + k_{437}$   
 $0xd5 = k_{127} + k_{128} + k_{137} + k_{138} + k_{142} + k_{145} + k_{146} + k_{212} + k_{214} + k_{215} + k_{216} + k_{218} + k_{222} + k_{225} + k_{226} + k_{414} + k_{418} + k_{434} + k_{438}$   
 $0xfa = k_{128} + k_{138} + k_{143} + k_{146} + k_{147} + k_{211} + k_{213} + k_{215} + k_{216} + k_{217} + k_{223} + k_{226} + k_{227} + k_{411} + k_{415} + k_{431} + k_{435}$   
 $0x39 = k_{141} + k_{142} + k_{144} + k_{146} + k_{148} + k_{212} + k_{213} + k_{217} + k_{218} + k_{222} + k_{224} + k_{226} + k_{228} + k_{231} + k_{411} + k_{413} + k_{414} + k_{416} + k_{417} + k_{431} + k_{433} + k_{434} + k_{436} + k_{437}$   
 $0x35 = k_{142} + k_{143} + k_{144} + k_{145} + k_{146} + k_{147} + k_{211} + k_{213} + k_{216} + k_{221} + k_{222} + k_{223} + k_{225} + k_{226} + k_{227} + k_{231} + k_{234} + k_{411} + k_{412} + k_{414} +$

$k_{415} + k_{417} + k_{431} + k_{432} + k_{434} + k_{435} + k_{437}$   
 $0x4b = k_{143} + k_{144} + k_{145} + k_{146} + k_{147} + k_{148} + k_{211} + k_{212} + k_{214} + k_{217} +$   
 $k_{221} + k_{222} + k_{223} + k_{224} + k_{225} + k_{226} + k_{227} + k_{228} + k_{231} + k_{232} + k_{411} +$   
 $k_{412} + k_{413} + k_{415} + k_{416} + k_{418} + k_{431} + k_{432} + k_{433} + k_{435} + k_{436} + k_{438}$   
 $0xe7 = k_{144} + k_{146} + k_{147} + k_{148} + k_{211} + k_{212} + k_{213} + k_{215} + k_{218} +$   
 $k_{222} + k_{223} + k_{224} + k_{226} + k_{227} + k_{228} + k_{232} + k_{233} + k_{411} + k_{412} + k_{413} +$   
 $k_{414} + k_{415} + k_{416} + k_{417} + k_{431} + k_{432} + k_{433} + k_{434} + k_{435} + k_{436} + k_{437}$   
 $0x33 = k_{145} + k_{146} + k_{212} + k_{213} + k_{214} + k_{216} + k_{221} + k_{225} + k_{226} + k_{231} +$   
 $k_{311} + k_{412} + k_{413} + k_{414} + k_{415} + k_{432} + k_{433} + k_{434} + k_{435} + k_{511} + k_{521}$   
 $0xdb = k_{146} + k_{147} + k_{213} + k_{214} + k_{217} + k_{222} + k_{226} + k_{227} + k_{232} +$   
 $k_{312} + k_{413} + k_{414} + k_{416} + k_{433} + k_{434} + k_{436} + k_{512} + k_{522}$   
 $0x8f = k_{147} + k_{148} + k_{211} + k_{213} + k_{214} + k_{215} + k_{216} + k_{217} + k_{221} +$   
 $k_{222} + k_{224} + k_{227} + k_{228} + k_{231} + k_{232} + k_{234} + k_{311} + k_{312} + k_{314} + k_{411} +$   
 $k_{413} + k_{414} + k_{415} + k_{416} + k_{418} + k_{431} + k_{433} + k_{434} + k_{435} + k_{436} + k_{438} +$   
 $k_{511} + k_{512} + k_{514} + k_{521} + k_{522} + k_{524}$   
 $0x83 = k_{148} + k_{212} + k_{214} + k_{215} + k_{216} + k_{217} + k_{218} + k_{221} + k_{222} + k_{223} +$   
 $k_{228} + k_{231} + k_{232} + k_{233} + k_{311} + k_{312} + k_{313} + k_{412} + k_{414} + k_{415} + k_{416} +$   
 $k_{417} + k_{432} + k_{434} + k_{435} + k_{436} + k_{437} + k_{511} + k_{512} + k_{513} + k_{521} + k_{522} + k_{523}$   
 $0x00 = k_{211} + k_{311} + k_{411} + k_{431} + k_{441}$   
 $0x00 = k_{212} + k_{312} + k_{412} + k_{432} + k_{442}$   
 $0x00 = k_{213} + k_{313} + k_{413} + k_{433} + k_{443}$   
 $0x00 = k_{214} + k_{314} + k_{414} + k_{434} + k_{444}$   
 $0x1f = k_{215} + k_{217} + k_{222} + k_{223} + k_{224} + k_{225} + k_{232} + k_{233} + k_{234} + k_{235} +$   
 $k_{311} + k_{312} + k_{313} + k_{314} + k_{415} + k_{417} + k_{435} + k_{437} + k_{441} + k_{442} + k_{443} + k_{444}$   
 $0x8e = k_{216} + k_{217} + k_{218} + k_{222} + k_{225} + k_{226} + k_{232} + k_{235} + k_{236} +$   
 $k_{311} + k_{416} + k_{417} + k_{418} + k_{436} + k_{437} + k_{438} + k_{441}$   
 $0x68 = k_{217} + k_{218} + k_{223} + k_{226} + k_{227} + k_{233} + k_{236} + k_{237} + k_{312} +$   
 $k_{417} + k_{418} + k_{437} + k_{438} + k_{442}$   
 $0x35 = k_{218} + k_{221} + k_{224} + k_{225} + k_{227} + k_{228} + k_{231} + k_{234} + k_{235} +$   
 $k_{237} + k_{238} + k_{313} + k_{418} + k_{438} + k_{443}$   
 $0x42 = k_{221} + k_{222} + k_{226} + k_{228} + k_{231} + k_{232} + k_{236} + k_{238} + k_{311} +$   
 $k_{314} + k_{315} + k_{441} + k_{444} + k_{445}$   
 $0xe6 = k_{222} + k_{223} + k_{225} + k_{227} + k_{232} + k_{233} + k_{235} + k_{237} + k_{311} +$   
 $k_{312} + k_{316} + k_{441} + k_{442} + k_{446}$   
 $0x91 = k_{223} + k_{224} + k_{226} + k_{233} + k_{234} + k_{236} + k_{312} + k_{313} + k_{314} +$   
 $k_{315} + k_{316} + k_{318} + k_{442} + k_{443} + k_{444} + k_{445} + k_{446} + k_{448}$   
 $0xf9 = k_{224} + k_{227} + k_{234} + k_{237} + k_{313} + k_{314} + k_{315} + k_{316} + k_{317} +$   
 $k_{443} + k_{444} + k_{445} + k_{446} + k_{447}$   
 $0xa0 = k_{225} + k_{228} + k_{235} + k_{238} + k_{311} + k_{313} + k_{315} + k_{444} + k_{511} +$

$k_{513} + k_{514} + k_{515} + k_{521} + k_{523} + k_{524} + k_{525}$   
 $0xb7 = k_{226} + k_{228} + k_{236} + k_{238} + k_{312} + k_{313} + k_{314} + k_{315} + k_{316} + k_{441} +$   
 $k_{444} + k_{511} + k_{512} + k_{513} + k_{515} + k_{516} + k_{521} + k_{522} + k_{523} + k_{525} + k_{526}$   
 $0x07 = k_{227} + k_{228} + k_{237} + k_{238} + k_{311} + k_{314} + k_{315} + k_{316} + k_{317} +$   
 $k_{441} + k_{442} + k_{444} + k_{512} + k_{515} + k_{516} + k_{517} + k_{522} + k_{525} + k_{526} + k_{527}$   
 $0xc1 = k_{228} + k_{238} + k_{311} + k_{312} + k_{315} + k_{316} + k_{317} + k_{318} + k_{441} + k_{442} +$   
 $k_{443} + k_{513} + k_{515} + k_{516} + k_{517} + k_{518} + k_{523} + k_{525} + k_{526} + k_{527} + k_{528}$   
 $0xc9 = k_{241} + k_{311} + k_{312} + k_{313} + k_{316} + k_{317} + k_{321} + k_{441} + k_{442} +$   
 $k_{443} + k_{447} + k_{448} + k_{511} + k_{516} + k_{518} + k_{521} + k_{526} + k_{528}$   
 $0xed = k_{242} + k_{311} + k_{312} + k_{313} + k_{314} + k_{315} + k_{317} + k_{318} + k_{322} +$   
 $k_{441} + k_{442} + k_{443} + k_{444} + k_{448} + k_{512} + k_{515} + k_{517} + k_{522} + k_{525} + k_{527}$   
 $0xf6 = k_{243} + k_{312} + k_{313} + k_{314} + k_{316} + k_{318} + k_{323} + k_{442} + k_{443} +$   
 $k_{444} + k_{445} + k_{513} + k_{515} + k_{518} + k_{521} + k_{525} + k_{526} + k_{528}$   
 $0x46 = k_{244} + k_{311} + k_{312} + k_{314} + k_{315} + k_{316} + k_{324} + k_{441} + k_{442} + k_{444} +$   
 $k_{446} + k_{447} + k_{448} + k_{514} + k_{515} + k_{517} + k_{518} + k_{524} + k_{525} + k_{527} + k_{528}$   
 $0x81 = k_{245} + k_{311} + k_{314} + k_{315} + k_{316} + k_{317} + k_{318} + k_{325} + k_{441} +$   
 $k_{443} + k_{446} + k_{448} + k_{513} + k_{514} + k_{517} + k_{523} + k_{524} + k_{527}$   
 $0x29 = k_{246} + k_{311} + k_{312} + k_{316} + k_{317} + k_{318} + k_{326} + k_{441} + k_{442} +$   
 $k_{444} + k_{445} + k_{447} + k_{514} + k_{515} + k_{518} + k_{524} + k_{525} + k_{528}$   
 $0x85 = k_{247} + k_{312} + k_{313} + k_{317} + k_{318} + k_{327} + k_{441} + k_{442} + k_{443} +$   
 $k_{445} + k_{446} + k_{448} + k_{511} + k_{515} + k_{516} + k_{521} + k_{525} + k_{526}$   
 $0x69 = k_{248} + k_{313} + k_{315} + k_{316} + k_{317} + k_{328} + k_{442} + k_{444} + k_{445} +$   
 $k_{447} + k_{448} + k_{512} + k_{513} + k_{514} + k_{516} + k_{522} + k_{523} + k_{524} + k_{526}$   
 $0x7b = k_{311} + k_{313} + k_{316} + k_{317} + k_{318} + k_{441} + k_{441} + k_{443} + k_{516} +$   
 $k_{517} + k_{518} + k_{526} + k_{527} + k_{528} + k_{541}$   
 $0x1b = k_{312} + k_{313} + k_{314} + k_{316} + k_{441} + k_{442} + k_{443} + k_{444} +$   
 $k_{516} + k_{526} + k_{541} + k_{542}$   
 $0xbc = k_{313} + k_{314} + k_{317} + k_{442} + k_{443} + k_{444} + k_{517} + k_{527} +$   
 $k_{542} + k_{543}$   
 $0x53 = k_{314} + k_{315} + k_{318} + k_{441} + k_{443} + k_{444} + k_{515} + k_{518} +$   
 $k_{525} + k_{528} + k_{541} + k_{543} + k_{544}$   
 $0x04 = k_{315} + k_{317} + k_{441} + k_{442} + k_{443} + k_{445} + k_{441} + k_{444} + k_{445} +$   
 $k_{446} + k_{447} + k_{448} + k_{511} + k_{514} + k_{516} + k_{518} + k_{521} + k_{524} + k_{526} + k_{528} +$   
 $k_{541} + k_{542} + k_{543} + k_{545}$   
 $0xcf = k_{316} + k_{317} + k_{318} + k_{444} + k_{445} + k_{446} + k_{442} + k_{444} + k_{445} +$   
 $k_{512} + k_{514} + k_{515} + k_{516} + k_{517} + k_{518} + k_{522} + k_{524} + k_{525} + k_{526} + k_{527} +$   
 $k_{528} + k_{544} + k_{545} + k_{546}$   
 $0x58 = k_{317} + k_{318} + k_{441} + k_{446} + k_{447} + k_{441} + k_{443} + k_{446} + k_{511} + k_{513} +$   
 $k_{516} + k_{517} + k_{518} + k_{521} + k_{523} + k_{526} + k_{527} + k_{528} + k_{541} + k_{546} + k_{547}$

$$\begin{aligned}
0x21 &= k_{318} + k_{412} + k_{415} + k_{417} + k_{418} + k_{441} + k_{442} + k_{444} + k_{447} + \\
&k_{511} + k_{512} + k_{514} + k_{517} + k_{518} + k_{521} + k_{522} + k_{524} + k_{527} + k_{528} + k_{542} + \\
&k_{545} + k_{547} + k_{548} \\
0x37 &= k_{321} + k_{331} + k_{411} + k_{412} + k_{413} + k_{414} + k_{416} + k_{417} + k_{418} + \\
&k_{441} + k_{444} + k_{445} + k_{447} + k_{511} + k_{514} + k_{515} + k_{517} + k_{521} + k_{524} + k_{525} + \\
&k_{527} + k_{541} + k_{542} + k_{543} + k_{544} + k_{546} + k_{547} + k_{548} \\
0xa3 &= k_{322} + k_{332} + k_{412} + k_{413} + k_{414} + k_{417} + k_{418} + k_{441} + k_{442} + \\
&k_{445} + k_{446} + k_{448} + k_{511} + k_{512} + k_{515} + k_{516} + k_{518} + k_{521} + k_{522} + k_{525} + \\
&k_{526} + k_{528} + k_{542} + k_{543} + k_{544} + k_{547} + k_{548} \\
0x9b &= k_{323} + k_{333} + k_{413} + k_{414} + k_{418} + k_{442} + k_{443} + k_{445} + k_{446} + \\
&k_{447} + k_{512} + k_{513} + k_{515} + k_{516} + k_{517} + k_{522} + k_{523} + k_{525} + k_{526} + k_{527} + \\
&k_{543} + k_{544} + k_{548} \\
0x51 &= k_{324} + k_{334} + k_{411} + k_{412} + k_{413} + k_{415} + k_{416} + k_{417} + k_{418} + \\
&k_{443} + k_{446} + k_{448} + k_{513} + k_{516} + k_{518} + k_{523} + k_{526} + k_{528} + k_{541} + k_{542} + \\
&k_{543} + k_{545} + k_{546} + k_{547} + k_{548} \\
0x4a &= k_{325} + k_{335} + k_{412} + k_{414} + k_{416} + k_{417} + k_{418} + k_{441} + k_{446} + k_{447} + \\
&k_{511} + k_{516} + k_{517} + k_{521} + k_{526} + k_{527} + k_{542} + k_{544} + k_{546} + k_{547} + k_{548} \\
0x5f &= k_{326} + k_{336} + k_{411} + k_{413} + k_{417} + k_{418} + k_{442} + k_{445} + k_{447} + k_{448} + \\
&k_{512} + k_{515} + k_{517} + k_{518} + k_{522} + k_{525} + k_{527} + k_{528} + k_{541} + k_{543} + k_{547} + k_{548} \\
0x9a &= k_{327} + k_{337} + k_{411} + k_{412} + k_{414} + k_{418} + k_{443} + k_{446} + k_{448} + \\
&k_{513} + k_{516} + k_{518} + k_{523} + k_{526} + k_{528} + k_{541} + k_{542} + k_{544} + k_{548} \\
0xc2 &= k_{328} + k_{338} + k_{411} + k_{413} + k_{414} + k_{415} + k_{416} + k_{417} + k_{418} + \\
&k_{444} + k_{445} + k_{446} + k_{514} + k_{515} + k_{516} + k_{524} + k_{525} + k_{526} + k_{541} + k_{543} + \\
&k_{544} + k_{545} + k_{546} + k_{547} + k_{548} \\
0x72 &= k_{341} + k_{414} + k_{418} + k_{431} + k_{443} + k_{447} + k_{513} + k_{517} + k_{523} + \\
&k_{527} + k_{541} + k_{544} + k_{548} \\
0xa2 &= k_{342} + k_{411} + k_{415} + k_{432} + k_{441} + k_{444} + k_{445} + k_{448} + k_{511} + \\
&k_{514} + k_{515} + k_{518} + k_{521} + k_{524} + k_{525} + k_{528} + k_{541} + k_{542} + k_{545} \\
0x68 &= k_{343} + k_{412} + k_{416} + k_{433} + k_{441} + k_{442} + k_{445} + k_{446} + k_{511} + \\
&k_{512} + k_{515} + k_{518} + k_{521} + k_{522} + k_{525} + k_{526} + k_{542} + k_{543} + k_{546} \\
0x56 &= k_{344} + k_{413} + k_{414} + k_{417} + k_{418} + k_{434} + k_{442} + k_{446} + k_{512} + \\
&k_{516} + k_{522} + k_{526} + k_{543} + k_{547} + k_{548} \\
0x80 &= k_{345} + k_{412} + k_{413} + k_{416} + k_{418} + k_{435} + k_{442} + k_{443} + k_{447} + \\
&k_{512} + k_{513} + k_{517} + k_{522} + k_{523} + k_{527} + k_{542} + k_{543} + k_{545} + k_{546} + k_{548} \\
0xda &= k_{346} + k_{411} + k_{413} + k_{414} + k_{415} + k_{417} + k_{436} + k_{441} + k_{443} + \\
&k_{444} + k_{445} + k_{448} + k_{511} + k_{513} + k_{514} + k_{515} + k_{518} + k_{521} + k_{523} + k_{524} + \\
&k_{525} + k_{528} + k_{541} + k_{543} + k_{544} + k_{545} + k_{546} + k_{547} \\
0xc7 &= k_{347} + k_{412} + k_{414} + k_{415} + k_{416} + k_{418} + k_{437} + k_{442} + k_{444} + \\
&k_{445} + k_{446} + k_{512} + k_{514} + k_{515} + k_{516} + k_{522} + k_{524} + k_{525} + k_{526} + k_{542} +
\end{aligned}$$

$$k_{544} + k_{545} + k_{546} + k_{547} + k_{548}$$

$$0x2c = k_{348} + k_{411} + k_{412} + k_{415} + k_{417} + k_{418} + k_{438} + k_{441} + k_{442} + k_{446} + k_{511} + k_{512} + k_{516} + k_{521} + k_{522} + k_{526} + k_{541} + k_{542} + k_{545} + k_{547}$$

$$0x5e = k_{411} + k_{413} + k_{414} + k_{415} + k_{416} + k_{417} + k_{418} + k_{441} + k_{444} + k_{446} + k_{448} + k_{514} + k_{516} + k_{518} + k_{521} + k_{524} + k_{526} + k_{528} + k_{541} + k_{543} + k_{544} + k_{545} + k_{546} + k_{547} + k_{548} + k_{611} + k_{631}$$

$$0x69 = k_{412} + k_{414} + k_{416} + k_{417} + k_{418} + k_{441} + k_{442} + k_{445} + k_{447} + k_{511} + k_{515} + k_{517} + k_{521} + k_{522} + k_{525} + k_{527} + k_{542} + k_{544} + k_{546} + k_{547} + k_{548} + k_{612} + k_{632}$$

$$0x66 = k_{413} + k_{414} + k_{415} + k_{418} + k_{441} + k_{442} + k_{443} + k_{448} + k_{511} + k_{513} + k_{514} + k_{518} + k_{521} + k_{522} + k_{523} + k_{528} + k_{543} + k_{544} + k_{545} + k_{548} + k_{612} + k_{614} + k_{632} + k_{634}$$

$$0x94 = k_{414} + k_{415} + k_{418} + k_{441} + k_{442} + k_{443} + k_{444} + k_{445} + k_{512} + k_{514} + k_{515} + k_{521} + k_{522} + k_{523} + k_{524} + k_{525} + k_{544} + k_{545} + k_{546} + k_{611} + k_{613} + k_{631} + k_{633}$$

$$0x8f = k_{415} + k_{416} + k_{441} + k_{442} + k_{443} + k_{444} + k_{515} + k_{521} + k_{522} + k_{523} + k_{524} + k_{545} + k_{546} + k_{611} + k_{612} + k_{613} + k_{614} + k_{615} + k_{631} + k_{632} + k_{633} + k_{634} + k_{635}$$

$$0x1b = k_{416} + k_{417} + k_{442} + k_{443} + k_{444} + k_{516} + k_{522} + k_{523} + k_{524} + k_{546} + k_{547} + k_{612} + k_{613} + k_{614} + k_{616} + k_{632} + k_{633} + k_{634} + k_{636}$$

$$0x48 = k_{417} + k_{418} + k_{442} + k_{443} + k_{515} + k_{516} + k_{518} + k_{522} + k_{523} + k_{547} + k_{548} + k_{612} + k_{613} + k_{615} + k_{618} + k_{632} + k_{633} + k_{635} + k_{636} + k_{638}$$

$$0x28 = k_{418} + k_{441} + k_{443} + k_{444} + k_{515} + k_{516} + k_{517} + k_{521} + k_{523} + k_{524} + k_{548} + k_{611} + k_{613} + k_{614} + k_{615} + k_{616} + k_{617} + k_{631} + k_{633} + k_{634} + k_{635} + k_{636} + k_{637}$$

$$0x00 = k_{421} + k_{431} + k_{445} + k_{525} + k_{615} + k_{635}$$

$$0x00 = k_{422} + k_{432} + k_{446} + k_{526} + k_{616} + k_{636}$$

$$0x00 = k_{423} + k_{433} + k_{447} + k_{527} + k_{617} + k_{637}$$

$$0x00 = k_{424} + k_{434} + k_{448} + k_{528} + k_{618} + k_{638}$$

$$0x00 = k_{425} + k_{435} + k_{441} + k_{521} + k_{611} + k_{631}$$

$$0x00 = k_{426} + k_{436} + k_{442} + k_{522} + k_{612} + k_{632}$$

$$0x00 = k_{427} + k_{437} + k_{443} + k_{523} + k_{613} + k_{633}$$

$$0x00 = k_{428} + k_{438} + k_{444} + k_{524} + k_{614} + k_{634}$$

$$0x7b = k_{441} + k_{443} + k_{516} + k_{517} + k_{518} + k_{521} + k_{523} + k_{545} + k_{611} + k_{613} + k_{616} + k_{617} + k_{618} + k_{631} + k_{633} + k_{636} + k_{637} + k_{638} + k_{645}$$

$$0x1b = k_{442} + k_{443} + k_{444} + k_{516} + k_{522} + k_{523} + k_{524} + k_{545} + k_{546} + k_{612} + k_{613} + k_{614} + k_{616} + k_{632} + k_{633} + k_{634} + k_{636} + k_{645} + k_{646}$$

$$0xbc = k_{443} + k_{444} + k_{517} + k_{523} + k_{524} + k_{546} + k_{547} + k_{613} + k_{617} + k_{633} + k_{634} + k_{646} + k_{647}$$

$0x53 = k4_{44} + k5_{15} + k5_{18} + k5_{24} + k5_{45} + k5_{47} + k5_{48} + k6_{14} + k6_{15} + k6_{18} + k6_{34} + k6_{35} + k6_{38} + k6_{45} + k6_{47} + k6_{48}$   
 $0x79 = k4_{45} + k4_{46} + k4_{47} + k5_{13} + k5_{25} + k5_{26} + k5_{27} + k5_{41} + k6_{13} + k6_{15} + k6_{16} + k6_{17} + k6_{33} + k6_{35} + k6_{36} + k6_{37} + k6_{41}$   
 $0xd8 = k4_{46} + k4_{47} + k4_{48} + k5_{11} + k5_{12} + k5_{26} + k5_{27} + k5_{28} + k5_{43} + k6_{11} + k6_{12} + k6_{16} + k6_{17} + k6_{18} + k6_{31} + k6_{32} + k6_{36} + k6_{37} + k6_{38} + k6_{43}$   
 $0xfb = k4_{47} + k4_{48} + k5_{12} + k5_{13} + k5_{27} + k5_{28} + k5_{41} + k5_{44} + k6_{12} + k6_{13} + k6_{17} + k6_{18} + k6_{32} + k6_{33} + k6_{37} + k6_{38} + k6_{41} + k6_{44}$   
 $0xba = k4_{48} + k5_{11} + k5_{13} + k5_{14} + k5_{28} + k5_{41} + k5_{42} + k6_{11} + k6_{13} + k6_{14} + k6_{18} + k6_{31} + k6_{33} + k6_{34} + k6_{38} + k6_{41} + k6_{42}$   
 $0x04 = k5_{11} + k5_{14} + k5_{15} + k5_{44} + k5_{45} + k5_{48} + k6_{11} + k6_{14} + k6_{15} + k6_{31} + k6_{34} + k6_{35} + k6_{43} + k6_{44} + k6_{45} + k6_{48} + k7_{13} + k7_{23}$   
 $0x25 = k5_{12} + k5_{17} + k5_{18} + k5_{42} + k5_{43} + k5_{44} + k5_{46} + k6_{12} + k6_{17} + k6_{18} + k6_{32} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{46} + k7_{11} + k7_{21}$   
 $0x96 = k5_{13} + k5_{18} + k5_{43} + k5_{44} + k5_{47} + k6_{13} + k6_{18} + k6_{33} + k6_{38} + k6_{42} + k6_{43} + k6_{44} + k6_{47} + k7_{12} + k7_{22}$   
 $0xca = k5_{14} + k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{42} + k5_{43} + k5_{48} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{34} + k6_{35} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k6_{48} + k7_{13} + k7_{14} + k7_{23} + k7_{24}$   
 $0x94 = k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{44} + k5_{48} + k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{35} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{21} + k7_{23} + k7_{24} + k7_{31}$   
 $0xa7 = k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{42} + k5_{45} + k6_{16} + k6_{17} + k6_{18} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k6_{45} + k7_{14} + k7_{22} + k7_{24} + k7_{32}$   
 $0xef = k5_{17} + k5_{18} + k5_{42} + k5_{43} + k5_{46} + k6_{17} + k6_{18} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{46} + k7_{11} + k7_{21} + k7_{23} + k7_{33}$   
 $0xc7 = k5_{18} + k5_{41} + k5_{43} + k5_{44} + k5_{47} + k6_{18} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{47} + k7_{12} + k7_{21} + k7_{22} + k7_{24} + k7_{31} + k7_{34}$   
 $0x69 = k5_{21} + k5_{31} + k5_{41} + k5_{43} + k5_{44} + k6_{41} + k6_{43} + k6_{44} + k7_{22} + k7_{32}$   
 $0xca = k5_{22} + k5_{32} + k5_{42} + k5_{44} + k6_{42} + k6_{44} + k7_{23} + k7_{33}$   
 $0x51 = k5_{23} + k5_{33} + k5_{41} + k5_{43} + k6_{41} + k6_{43} + k7_{21} + k7_{24} + k7_{31} + k7_{34}$   
 $0x5e = k5_{24} + k5_{34} + k5_{42} + k5_{43} + k6_{42} + k6_{43} + k7_{21} + k7_{31}$   
 $0x33 = k5_{25} + k5_{35} + k5_{42} + k5_{44} + k5_{48} + k6_{42} + k6_{43} + k6_{44} + k6_{48} + k7_{13} + k7_{21} + k7_{22} + k7_{23} + k7_{31} + k7_{32}$   
 $0x48 = k5_{26} + k5_{36} + k5_{41} + k5_{43} + k5_{45} + k6_{43} + k6_{44} + k6_{45} + k7_{11} + k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33}$   
 $0x28 = k5_{27} + k5_{37} + k5_{41} + k5_{42} + k5_{44} + k5_{46} + k6_{44} + k6_{46} + k7_{11} + k7_{12} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34}$   
 $0xc7 = k5_{28} + k5_{38} + k5_{41} + k5_{43} + k5_{44} + k5_{47} + k5_{48} + k6_{41} + k6_{42} +$

$k6_{43} + k6_{44} + k6_{47} + k6_{48} + k7_{12} + k7_{21} + k7_{22} + k7_{24} + k7_{31} + k7_{34}$   
 $0x09 = k5_{41} + k5_{42} + k5_{43} + k5_{44} + k6_{11} + k6_{41} + k6_{42} + k7_{13} + k7_{14} +$   
 $k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{32} + k7_{41}$   
 $0x16 = k5_{42} + k5_{43} + k5_{44} + k6_{12} + k6_{42} + k6_{43} + k7_{14} + k7_{22} + k7_{23} +$   
 $k7_{24} + k7_{32} + k7_{33} + k7_{42}$   
 $0xde = k5_{43} + k5_{44} + k6_{13} + k6_{41} + k6_{43} + k6_{44} + k7_{11} + k7_{23} + k7_{24} +$   
 $k7_{31} + k7_{33} + k7_{34} + k7_{43}$   
 $0x2c = k5_{44} + k6_{11} + k6_{14} + k6_{42} + k6_{44} + k7_{12} + k7_{24} + k7_{32} + k7_{34} +$   
 $k7_{41} + k7_{44}$   
 $0x02 = k5_{45} + k5_{47} + k6_{12} + k6_{13} + k6_{14} + k6_{16} + k6_{42} + k6_{43} + k6_{44} + k6_{45} +$   
 $k6_{47} + k7_{12} + k7_{13} + k7_{14} + k7_{22} + k7_{23} + k7_{34} + k7_{42} + k7_{43} + k7_{44} + k7_{46}$   
 $0x43 = k5_{46} + k5_{48} + k6_{11} + k6_{12} + k6_{13} + k6_{14} + k6_{15} + k6_{41} + k6_{42} +$   
 $k6_{43} + k6_{44} + k6_{46} + k6_{48} + k7_{11} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{22} + k7_{33} +$   
 $k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{45}$   
 $0x7d = k5_{47} + k6_{11} + k6_{13} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{41} + k6_{43} +$   
 $k6_{44} + k6_{47} + k7_{11} + k7_{13} + k7_{14} + k7_{24} + k7_{31} + k7_{33} + k7_{41} + k7_{43} + k7_{44} +$   
 $k7_{45} + k7_{46} + k7_{47}$   
 $0x57 = k5_{48} + k6_{11} + k6_{14} + k6_{16} + k6_{18} + k6_{41} + k6_{44} + k6_{48} + k7_{11} +$   
 $k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{41} + k7_{44} + k7_{46} + k7_{48}$   
 $0x37 = k6_{11} + k6_{14} + k6_{22} + k6_{32} + k6_{42} + k7_{12} + k7_{21} + k7_{22} + k7_{31} +$   
 $k7_{41} + k7_{44}$   
 $0x94 = k6_{12} + k6_{14} + k6_{22} + k6_{23} + k6_{32} + k6_{33} + k6_{42} + k6_{43} + k7_{12} +$   
 $k7_{13} + k7_{21} + k7_{23} + k7_{31} + k7_{32} + k7_{42} + k7_{44}$   
 $0x51 = k6_{13} + k6_{21} + k6_{31} + k6_{41} + k7_{11} + k7_{21} + k7_{24} + k7_{34} + k7_{43}$   
 $0x5e = k6_{14} + k6_{22} + k6_{23} + k6_{24} + k6_{32} + k6_{33} + k6_{34} + k6_{42} + k6_{43} +$   
 $k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{31} + k7_{32} + k7_{33} + k7_{34} + k7_{44}$   
 $0x33 = k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{22} + k6_{24} + k6_{25} + k6_{32} + k6_{34} +$   
 $k6_{35} + k6_{41} + k7_{11} + k7_{21} + k7_{45} + k7_{46} + k7_{47} + k7_{48}$   
 $0x48 = k6_{16} + k6_{17} + k6_{18} + k6_{21} + k6_{23} + k6_{26} + k6_{31} + k6_{33} + k6_{36} +$   
 $k6_{42} + k7_{12} + k7_{22} + k7_{46} + k7_{47} + k7_{48}$   
 $0x28 = k6_{17} + k6_{18} + k6_{21} + k6_{22} + k6_{24} + k6_{27} + k6_{31} + k6_{32} + k6_{34} +$   
 $k6_{37} + k6_{43} + k7_{13} + k7_{23} + k7_{47} + k7_{48}$   
 $0xf4 = k6_{18} + k6_{21} + k6_{22} + k6_{23} + k6_{25} + k6_{28} + k6_{31} + k6_{32} + k6_{33} +$   
 $k6_{35} + k6_{38} + k6_{41} + k6_{44} + k7_{11} + k7_{14} + k7_{21} + k7_{24} + k7_{48}$   
 $0xf7 = k6_{21} + k6_{25} + k6_{31} + k6_{35} + k6_{41} + k7_{11} + k7_{22} + k7_{24} + k7_{31} +$   
 $k7_{32} + k7_{34} + k7_{43} + k8_{13} + k8_{23}$   
 $0xcc = k6_{22} + k6_{23} + k6_{24} + k6_{26} + k6_{27} + k6_{28} + k6_{32} + k6_{33} + k6_{34} +$   
 $k6_{36} + k6_{37} + k6_{38} + k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{22} +$   
 $k7_{31} + k7_{33} + k7_{34} + k7_{44} + k8_{14} + k8_{24}$

$0x52 = k6_{23} + k6_{24} + k6_{27} + k6_{28} + k6_{33} + k6_{34} + k6_{37} + k6_{38} + k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{22} + k7_{23} + k7_{32} + k7_{34} + k7_{41} + k8_{11} + k8_{21}$   
 $0xf8 = k6_{24} + k6_{28} + k6_{34} + k6_{38} + k6_{44} + k7_{14} + k7_{21} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{42} + k8_{12} + k8_{22}$   
 $0xf9 = k6_{25} + k6_{27} + k6_{28} + k6_{35} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k7_{11} + k7_{12} + k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{46} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{16} + k8_{21} + k8_{22} + k8_{23} + k8_{24} + k8_{26}$   
 $0x60 = k6_{26} + k6_{27} + k6_{36} + k6_{37} + k6_{41} + k6_{43} + k7_{11} + k7_{13} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{45} + k8_{11} + k8_{12} + k8_{13} + k8_{15} + k8_{21} + k8_{22} + k8_{23} + k8_{25}$   
 $0xc1 = k6_{27} + k6_{28} + k6_{37} + k6_{38} + k6_{42} + k7_{12} + k7_{21} + k7_{22} + k7_{31} + k7_{41} + k7_{44} + k7_{45} + k7_{47} + k8_{11} + k8_{14} + k8_{15} + k8_{17} + k8_{21} + k8_{24} + k8_{25} + k8_{27}$   
 $0xc0 = k6_{28} + k6_{38} + k6_{43} + k7_{13} + k7_{22} + k7_{23} + k7_{32} + k7_{41} + k7_{42} + k7_{45} + k7_{46} + k7_{48} + k8_{11} + k8_{12} + k8_{15} + k8_{16} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{26} + k8_{28}$   
 $0x2c = k6_{41} + k6_{43} + k7_{11} + k7_{13} + k7_{21} + k7_{22} + k7_{24} + k7_{32} + k7_{33} + k7_{34} + k7_{41} + k7_{43} + k7_{44} + k7_{45} + k8_{11} + k8_{13} + k8_{14} + k8_{15} + k8_{23} + k8_{24} + k8_{25} + k8_{31}$   
 $0xf5 = k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{23} + k7_{24} + k7_{32} + k7_{41} + k7_{42} + k7_{43} + k7_{45} + k7_{46} + k8_{11} + k8_{12} + k8_{13} + k8_{15} + k8_{16} + k8_{23} + k8_{25} + k8_{26} + k8_{31} + k8_{32}$   
 $0x08 = k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{24} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{46} + k7_{47} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{16} + k8_{17} + k8_{21} + k8_{24} + k8_{26} + k8_{27} + k8_{32} + k8_{33}$   
 $0xe9 = k6_{44} + k7_{14} + k7_{21} + k7_{31} + k7_{34} + k7_{42} + k7_{43} + k7_{44} + k7_{45} + k7_{47} + k7_{48} + k8_{12} + k8_{13} + k8_{14} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{27} + k8_{28} + k8_{31} + k8_{33} + k8_{34}$   
 $0xcd = k6_{45} + k7_{15} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{25} + k7_{31} + k7_{32} + k7_{33} + k7_{34} + k7_{41} + k7_{46} + k7_{48} + k8_{11} + k8_{16} + k8_{18} + k8_{22} + k8_{23} + k8_{26} + k8_{28} + k8_{31} + k8_{32} + k8_{33}$   
 $0xfd = k6_{46} + k7_{16} + k7_{22} + k7_{23} + k7_{24} + k7_{26} + k7_{32} + k7_{33} + k7_{34} + k7_{42} + k7_{45} + k7_{47} + k8_{12} + k8_{15} + k8_{17} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{27} + k8_{31} + k8_{32} + k8_{33} + k8_{34}$   
 $0xe1 = k6_{47} + k7_{17} + k7_{23} + k7_{24} + k7_{27} + k7_{33} + k7_{34} + k7_{43} + k7_{45} + k7_{46} + k7_{48} + k8_{13} + k8_{15} + k8_{16} + k8_{18} + k8_{22} + k8_{24} + k8_{25} + k8_{26} + k8_{28} + k8_{32} + k8_{33} + k8_{34}$   
 $0xe9 = k6_{48} + k7_{18} + k7_{21} + k7_{22} + k7_{23} + k7_{28} + k7_{31} + k7_{32} + k7_{33} + k7_{44} + k7_{45} + k7_{47} + k7_{48} + k8_{14} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{27} + k8_{28} + k8_{31} + k8_{32} + k8_{34}$   
 $0xa = k7_{11} + k7_{23} + k7_{24} + k7_{33} + k7_{34} + k7_{43} + k7_{44} + k8_{13} + k8_{14} + k8_{22} + k8_{32} + k8_{33} + k8_{34} + k8_{41}$

$0x0d = k7_{12} + k7_{24} + k7_{34} + k7_{44} + k8_{14} + k8_{23} + k8_{33} + k8_{34} + k8_{42}$   
 $0xe0 = k7_{13} + k7_{21} + k7_{31} + k7_{41} + k8_{11} + k8_{21} + k8_{24} + k8_{34} + k8_{43}$   
 $0xa4 = k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{34} + k7_{42} + k7_{43} +$   
 $k7_{44} + k8_{12} + k8_{13} + k8_{14} + k8_{21} + k8_{32} + k8_{33} + k8_{34} + k8_{44}$   
 $0x8c = k7_{15} + k7_{21} + k7_{22} + k7_{31} + k7_{32} + k7_{42} + k7_{43} + k7_{44} + k7_{45} +$   
 $k8_{12} + k8_{13} + k8_{14} + k8_{15} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{31} + k8_{32} + k8_{45}$   
 $0xdb = k7_{16} + k7_{22} + k7_{23} + k7_{32} + k7_{33} + k7_{43} + k7_{44} + k7_{46} + k8_{13} +$   
 $k8_{14} + k8_{16} + k8_{22} + k8_{24} + k8_{26} + k8_{32} + k8_{33} + k8_{46}$   
 $0x58 = k7_{17} + k7_{21} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34} + k7_{44} + k7_{47} +$   
 $k8_{14} + k8_{17} + k8_{21} + k8_{23} + k8_{27} + k8_{31} + k8_{33} + k8_{34} + k8_{47}$   
 $0x2e = k7_{18} + k7_{21} + k7_{24} + k7_{31} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{48} +$   
 $k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{18} + k8_{22} + k8_{23} + k8_{28} + k8_{31} + k8_{34} + k8_{48}$   
 $0x91 = k7_{21} + k7_{24} + k7_{31} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k8_{11} +$   
 $k8_{12} + k8_{13} + k8_{14} + k8_{23} + k8_{24} + k8_{26} + k8_{31} + k8_{32} + k8_{36}$   
 $0x68 = k7_{22} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k8_{11} + k8_{23} + k8_{26} + k8_{27} +$   
 $k8_{31} + k8_{33} + k8_{36} + k8_{37}$   
 $0x1f = k7_{23} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k8_{11} + k8_{12} + k8_{13} + k8_{22} +$   
 $k8_{23} + k8_{24} + k8_{25} + k8_{31} + k8_{34} + k8_{35}$   
 $0xbb = k7_{24} + k7_{34} + k7_{42} + k7_{44} + k8_{12} + k8_{14} + k8_{21} + k8_{22} + k8_{24} +$   
 $k8_{26} + k8_{27} + k8_{28} + k8_{31} + k8_{36} + k8_{37} + k8_{38}$   
 $0xe6 = k7_{25} + k7_{35} + k7_{45} + k7_{46} + k7_{47} + k7_{48} + k8_{15} + k8_{16} + k8_{17} +$   
 $k8_{18} + k8_{22} + k8_{23} + k8_{25} + k8_{27} + k8_{32} + k8_{33} + k8_{36} + k8_{38}$   
 $0x5d = k7_{26} + k7_{36} + k7_{46} + k7_{47} + k7_{48} + k8_{16} + k8_{17} + k8_{18} + k8_{21} +$   
 $k8_{23} + k8_{24} + k8_{25} + k8_{26} + k8_{28} + k8_{31} + k8_{33} + k8_{34} + k8_{35} + k8_{37}$   
 $0x77 = k7_{27} + k7_{37} + k7_{47} + k7_{48} + k8_{17} + k8_{18} + k8_{22} + k8_{24} + k8_{25} +$   
 $k8_{26} + k8_{27} + k8_{32} + k8_{34} + k8_{35} + k8_{36} + k8_{38}$   
 $0x42 = k7_{28} + k7_{38} + k7_{45} + k7_{46} + k7_{47} + k8_{15} + k8_{16} + k8_{17} + k8_{21} +$   
 $k8_{22} + k8_{26} + k8_{28} + k8_{31} + k8_{32} + k8_{35} + k8_{37} + k8_{38}$   
 $0x78 = k7_{41} + k7_{45} + k7_{46} + k7_{48} + k8_{11} + k8_{15} + k8_{16} + k8_{18} + k8_{22} +$   
 $k8_{24} + k8_{26} + k8_{31} + k8_{32} + k8_{34} + k8_{35} + k8_{38} + k8_{41} + k9_{11} + k9_{21}$   
 $0x85 = k7_{42} + k7_{45} + k7_{46} + k7_{47} + k8_{12} + k8_{15} + k8_{16} + k8_{17} + k8_{21} +$   
 $k8_{23} + k8_{27} + k8_{31} + k8_{32} + k8_{33} + k8_{35} + k8_{36} + k8_{42} + k9_{12} + k9_{22}$   
 $0x16 = k7_{43} + k7_{45} + k7_{46} + k7_{47} + k7_{48} + k8_{13} + k8_{15} + k8_{16} + k8_{17} +$   
 $k8_{18} + k8_{21} + k8_{22} + k8_{24} + k8_{25} + k8_{28} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{36} +$   
 $k8_{37} + k8_{43} + k9_{13} + k9_{23}$   
 $0x24 = k7_{44} + k7_{45} + k7_{47} + k8_{14} + k8_{15} + k8_{17} + k8_{21} + k8_{23} + k8_{24} +$   
 $k8_{25} + k8_{31} + k8_{33} + k8_{37} + k8_{44} + k9_{14} + k9_{24}$   
 $0x7c = k7_{45} + k7_{47} + k7_{48} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{26} +$   
 $k8_{27} + k8_{28} + k8_{31} + k8_{32} + k8_{36} + k8_{43} + k8_{46} + k9_{13} + k9_{16} + k9_{23} + k9_{26}$

$0x42 = k7_{46} + k7_{47} + k8_{16} + k8_{17} + k8_{21} + k8_{24} + k8_{25} + k8_{26} + k8_{27} + k8_{31} + k8_{34} + k8_{35} + k8_{42} + k8_{45} + k9_{12} + k9_{15} + k9_{22} + k9_{25}$

$0x5d = k7_{47} + k7_{48} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{23} + k8_{24} + k8_{25} + k8_{28} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{35} + k8_{37} + k8_{41} + k8_{42} + k8_{44} + k8_{45} + k8_{47} + k9_{11} + k9_{12} + k9_{14} + k9_{15} + k9_{17} + k9_{21} + k9_{22} + k9_{24} + k9_{25} + k9_{27}$

$0x56 = k7_{48} + k8_{18} + k8_{22} + k8_{23} + k8_{24} + k8_{25} + k8_{26} + k8_{32} + k8_{33} + k8_{34} + k8_{35} + k8_{36} + k8_{38} + k8_{41} + k8_{42} + k8_{43} + k8_{45} + k8_{46} + k8_{48} + k9_{11} + k9_{12} + k9_{13} + k9_{15} + k9_{16} + k9_{18} + k9_{21} + k9_{22} + k9_{23} + k9_{25} + k9_{26} + k9_{28}$

【0122】

ここで、下記式が成立する。

【0123】

【数40】

$$\text{rank } (M^*_{KH}) = N_m - N_r$$

【0124】

従って、上記168個の線形関係式は、互いに独立な線形関係式である。従つて、これら168個のGF(2)上の任意を線形結合して得られる $2^{168}-1$ 個の線形関係式が成り立つことがわかる。この線形関係式が多ければ、暗号の設計者の意図しない新たな攻撃を招く恐れがあるので、上述した方法によって得られた線形関係式の総数を、暗号強度評価の一つの指標として用いることができる。

【0125】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0126】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることができる。

【0127】

例えば、プログラムは記憶媒体としてのハードディスクやROM (Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0128】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体にインストールすることができる。

【0129】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的あるいは個別に実行されてもよい。

【0130】

【発明の効果】

以上、説明したように、本発明の構成によれば、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することが可能となり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を実行することが可能となる。

【0131】

本発明の構成によれば、暗号アルゴリズムのうち、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することにより、ラウン

ド鍵間の全ての線形関係式を求めることが可能となる。ラウンド鍵間に単純な依存関係が存在すると、実質的なラウンド鍵の数が減ってしまうことになるため、暗号の設計者は、このような関係式が多数存在することがないよう、注意する必要がある。本発明に係る方法によって、ラウンド鍵間の線形関係式の数が少なくなるよう、暗号鍵の強度を評価することによって、より安全な暗号を設計することが可能になる。

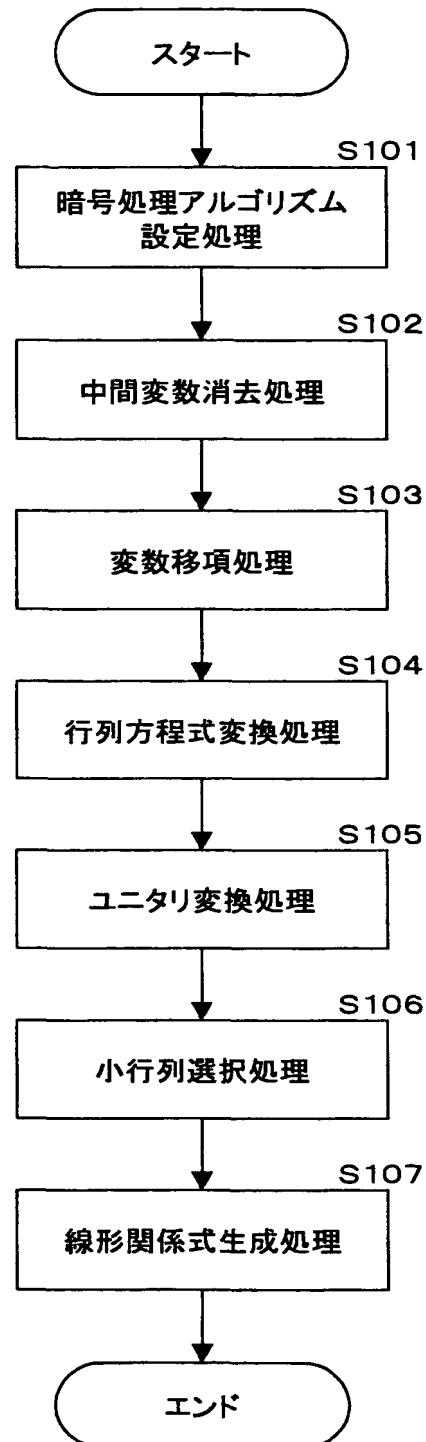
【図面の簡単な説明】

【図1】

本発明を適用した暗号強度指標算出処理手順を説明するフローチャートを示す図である。

【書類名】 図面

【図1】



【書類名】 要約書

【要約】

【課題】 共通鍵ブロック暗号における暗号強度評価処理を確実に実行する方法を提供する。

【解決手段】 共通鍵ブロック暗号アルゴリズムにおいて、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することにより、ラウンド鍵間の全ての線形関係式を求める。本方式によれば、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することが可能となり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を実行することが可能となる。

【選択図】 図1

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社